Canada Border Services Agency
Agence des services frontaliers du Canada

Scenario-Based Targeting Governance Framework

Targeting Program,
Enforcement and Intelligence
Programs Directorate

Programs Branch

2018-03-15

PROTECTION • SERVICE • INTEGRITY

Canada

PREAMBLE

The CBSA Scenario-Based Targeting Governance Framework was drafted by the Targeting Program Unit within the Enforcement and Intelligence Programs Directorate, Programs Branch.

This document has been verified for technical accuracy at the time of publication and requests for additional use must be vetted through the Targeting Program Unit. This document may not be reproduced or distributed without the permission of the Targeting Program Unit. This publication is not intended for external use.

If access is requested under the *Access to Information Act* or *Privacy Act*, no decisions should be taken without prior consultations with the Targeting Program Unit, as the requested information may be subject to exemptions.

Table of Contents

Scenario-Based Targeting Governance Framework

Introduction

The Targeting Program identifies people and goods bound for Canada that may pose a threat to the security and safety of the country. The Canada Border Services Agency (CBSA) receives advance information from commercial air carriers to identify people for pre-arrival risk assessment purposes. The requirement for commercial air carriers to provide Advance Passenger Information (API) and all available Passenger Name Record (PNR) data, concerning all travellers (including crew) to the CBSA before a flight's departure, comes from section 5(a)-(f) of the Passenger Information Customs Regulations (PICR) and section 269(1)(a)-(f) of the Immigration Refugee Protection Regulations (IRPR). API and PNR enables the CBSA to identify in advance people who may pose a risk to national security, may be involved in illicit migration, or the smuggling of contraband. Domestic law and international agreements restrict Canada's use of PNR data to preventing and detecting terrorism offences or serious transnational crime while limiting the impact on privacy, civil liberties and human rights.

The API/PNR data is automatically screened through pre-determined Scenario-Based Targeting (SBT) rules known as scenarios within the CBSA Passenger Information System (PAXIS). Scenarios are generated upon intelligence, emerging threats, and comparative enforcement analyses that are associated to terrorism offences or serious transnational crime including contraband or illicit migration.

When API/PNR is received by the CBSA, it is processed through all active scenarios. If the traveller's information matches all criteria of a scenario, the traveller is placed on the "Scenario Work List" in PAXIS. Targeting Officers at the National Targeting Centre (NTC) will conduct comprehensive reviews on travellers who have matched scenarios in order to confirm or negate the potential risk. In addition to the scenario match, the traveller's information is processed through a number of queries to various internal and external databases either automatically or manually, in order to provide supplemental information for use during the review by the Targeting Officer. If the risk is determined to be valid, a target will be issued which will enable the interception of the traveller for further processing upon arrival in Canada.

Background

The CBSA made a commitment to the Office of the Privacy Commissioner of Canada to establish a governance framework for the review of scenarios for effectiveness and proportionality and to ensure that the scenarios do not unnecessarily infringe upon the privacy, civil liberties or human rights of travellers.

CBSA Commitments

The CBSA adheres to all legislation and regulations with regard to the restrictions on the use of API and PNR, as defined in the *Protection of Passenger Information Regulations* (PPIR) and the *Passenger Information Customs Regulations* (PICR).

The consolidated requirements of the *PPIR, PICR,* and the strict program application guidelines can be found in the Directive Memorandum D1-16-3 *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and PNR Data*.

Civil Liberties & Human Rights

The program is responsible for ensuring each scenario component does not contain sensitive or personal data that may contravene the *Charter of Rights and Freedoms* or the *Canadian Human Rights Act.*

Civil liberties are the basic rights and freedoms granted to Canadian citizens as well as all foreign nationals on Canadian territory.

> Section 2 of the *Charter of Rights and Freedoms* guarantees everyone has the following fundamental freedoms: freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; freedom of peaceful assembly; and freedom of association.
>
> Section 15(1) of the *Charter of Rights and Freedoms* guarantees every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.
>
> Section 3 of the *Canadian Human Rights Act* states that the prohibited grounds of discrimination are race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.

In order to protect the civil liberties and human rights of travellers, the CBSA ensures that scenarios (including the trend analysis, API/PNR data elements, indicators, and scenario description derived from the trend analysis) do not contain any sensitive data as defined by the *Canada-European Union Passenger Name Record Agreement (CAN – EU PNR Agreement)*, which was developed having regard to the relevant provisions of the *Canadian Charter of Rights and Freedoms* and Canadian privacy legislation. Sensitive data is any information that could reveal:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Information about a person's health or sex life

A passenger's flight reservation may contain a Special Service Requirements (SSR) and/or a free text field which are part of the airline's Passenger Name Record (PNR) transmitted to the CBSA. As the SSR and/or free text field may contain "sensitive data", the CBSA's Data Acquisition Solution (DAS) purges these specific SSR data elements and those contained in the free text fields prior to displaying in PAXIS.

Minimal Privacy Intrusion

To minimize privacy intrusion, scenario descriptions or names cannot contain any information that may be considered sensitive data:

- meal preference (religious or philosophical beliefs / information about a person's health)
- family status (information about a person's sex life)
- disability requirements (information about a person's health)
- language (racial or ethnic origin)
- passport designation (political opinions)
- free text/information collected for analysis (applies to all sensitive data)
- birth city/country (racial or ethnic origin)

Scope of a Scenario

Scenarios are comprised of both API and PNR data elements. The use of PNR information is regulated by the PPIR; section 4(1) of the PPIR states:

> 4 (1) Subject to subsections (2) to (5), an official of the Agency may, for the following purposes, have access to any passenger name record information that is retained:
>
> (a) to identify persons who have or may have committed a terrorism offence or a serious transnational crime.
>
> (b) to conduct a trend analysis or develop risk indicators for the purpose referred to in paragraph (a).

API and PNR information will be used by the CBSA to target persons who will be subjected to closer questioning and/or examination upon arrival in Canada, or who require further investigation, for one of the purposes described above.

Meeting Regulatory Requirements: Terrorism Offences/Serious Transnational Crime

The Agency is permitted, as detailed in the *Protection of Passenger Information Regulations*, to use PNR for the purposes of identifying persons who have, or may have, committed terrorism offences or a serious transnational crime or to conduct trend analysis or develop risk indicators for the same purpose.

To meet regulatory requirements, each scenario must include the specific statutory authority (i.e., *Customs Act*, *Immigration and Refugee Protection Act*) that supports the creation of the scenario;

and, include a brief summary as to how the scenario meets the requirements. This information must always be included with the scenario to ensure throughout the life of the scenario there is always a link to the statute, legislation and regulation that supports it.

The scenario must focus on identifying individuals who have or may have committed a terrorism offence or serious transnational crime. The trend analysis, the PNR data elements, the indicators and the scenario description must be developed in accordance with the regulations and reflect the allowable purpose, for which it is created.

A scenario meets the regulatory requirements under the following conditions:

- the initial purpose of developing the scenario is supported by the regulations;
- the scope and use of the scenario is supported by the regulations; and
- each scenario is specifically developed for identifying terrorism offences or serious transnational crime.

Terrorism offence is defined in the PPIR as follows:

> Terrorism offence means
>
> (a) an act or omission that is committed for a political, religious or ideological purpose, objective or cause with the intention of intimidating the public with regard to its security, including its economic security, or with the intention of compelling a person, government or domestic or international organization to do or refrain from doing any act, and that is committed with the intention to
>
> - (i) cause death or serious bodily harm,
> - (ii) endanger a person's life,
> - (iii) cause a serious risk to the health or safety of the public,
> - (iv) cause substantial property damage that is likely to result in the harm referred to in any of subparagraphs (i) to (iii), or
> - (v) cause serious interference with or serious disruption of an essential service, facility or system other than as a result of lawful or unlawful advocacy, protest, dissent or stoppage of work, such as a strike, that is not intended to result in the harm referred to in any of subparagraphs (i) to (iii);
>
> (b) an act or omission referred to in paragraph (a) of the definition terrorist activity in subsection 83.01(1) of the Criminal Code;
>
> (c) knowingly participating in or contributing to an activity for the purpose of enhancing a terrorist group's ability to facilitate or commit an act or omission referred to in paragraph (a) or (b) or instructing a person, group or organization to carry out an activity for that purpose;
>
> (d) an indictable offence if the act or omission that constitutes the offence is committed for the benefit of, at the direction of or in association with a terrorist group;

(e) any of the following, if they are carried out for the purpose of committing an act or omission referred to in paragraph (a) or (b):

- (i) collecting, using or possessing property,
- (ii) providing or making available property or a financial or related service, or
- (iii) inviting a person, group or organization to provide property or a financial or related service;

(f) attempting or threatening to commit an act or omission referred to in paragraph (a) or (b);

(g) conspiring to commit, or facilitating, instructing or counselling the commission of, an act or omission referred to in paragraph (a) or (b);

(h) being an accessory after the fact to an act or omission referred to in paragraph (a) or (b); or

(i) harbouring or concealing for the purpose of enabling a terrorist group to facilitate or commit an act or omission referred to in paragraph (a) or (b). (terrorism offence)

Serious transnational crime is defined in the PPIR as follows:

> Serious transnational crime means an act or omission that constitutes an offence punishable in Canada by a maximum term of imprisonment of at least four years and that is committed
>
> (a) in more than one country;
>
> (b) in only one country but a substantial part of its preparation, planning, direction or control takes place in another country;
>
> (c) in only one country but an organized criminal group that engages in criminal activities in more than one country is implicated in the act or omission;
>
> (d) in only one country but has substantial effects in another country; or
>
> (e) in a country other than Canada but the offender intends to travel to or transit through Canada. (crime transnational grave)

Examples of serious transnational crime are included in paragraph 15 of Departmental Memorandum D1-16-3, *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and Passenger Name Record (PNR) Data*:

> 15. Examples of serious transnational crimes include, but are not limited to:
> (a) narcotics smuggling;
> (b) human smuggling;
> (c) human trafficking; and
> (d) importation or smuggling of child pornography.

Scenario Risk Categories & Legislative Authorities

The *Customs Act and* the *Immigration and Refugee Protection Act* (IRPA) are the primary legislative authorities that allow the CBSA to identify risks for National Security, Contraband and Illicit Migration.

A) National Security Scenarios:

i) National Security – Canadian Citizens (*Canada Border Services Act*, Sections 2 and 5)

The examination of Canadian Citizens for national security is limited to statutory provisions contained in the CBSA program legislation, as defined in section 2 of the CBSA Act, and the mandate of the Agency as established in section 5 of the CBSA Act.

ii) National Security – Goods (*Customs Act*, S. 159)

The legislative authority to risk assess, identify and intercept goods associated to national security risks is found in Section 159 of the *Customs Act*. National Security scenarios are developed using intelligence information, trend and threat analysis associated to the transportation of prohibited goods identified as terrorism propaganda (D9-1-18).

iii) Security – Foreign Nationals or Permanent Residents (IRPA Section 34 (1) (a – f))

National security scenarios identifying risks to 'Security' are designed using intelligence information and/or trend analysis that identifies foreign nationals or permanent residents who have or may have committed a terrorist offence and may be inadmissible under the IRPA Section 34 for those reasons.

B) Contraband Scenarios (*Customs Act*, S. 159):

The legislative authority to intercept contraband risks is Section 159 of the *Customs Act*. Contraband scenarios must be designed using previous enforcement actions/intelligence or partner information that identifies individuals who have or may have committed a serious transnational crime.

C) Illicit Migration Scenarios:

i) Human or International Rights Violations (IRPA Section 35 (1) (a – c))

Illicit migration scenarios identifying risks to 'Human or International Rights Violations' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents, who may have committed human or international rights violations, and, who have or may have committed a terrorist offence or a serious transnational crime and, may be inadmissible under the IRPA Section 35 for those reasons.

ii) Serious Criminality (IRPA Section 36 (1) (a – c) Section 36 (2) (a –c))

Illicit migration scenarios identifying risks to 'Serious Criminality' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents who have or may have committed a serious transnational crime and may be inadmissible under the IRPA Section 36 for those reasons.

iii) Organized Criminality (IRPA Section 37 (1) (a) (b))

Illicit migration scenarios identifying risks to 'Organized Criminality' must be designed using analysis of previous enforcement actions/intelligence or partner information that identifies foreign nationals or permanent residents who may belong or have belonged to an organized criminal group, who are known to have or may have committed a serious transnational crime and may be inadmissible under the IRPA Section 37 for those reasons.

iv) Human Smuggling (IRPA Section 117)

Illicit migration scenarios identifying 'human smuggling' risks must be designed using intelligence analysis that identifies foreign nationals who may be involved in illicit migration through the organized transport of a person across an international border (clandestine smuggling or fraudulent activities). The legislative authority related to human smuggling is included in section 117 of IRPA.

Illicit migration scenarios must focus on those that have or may have committed an offence linked to human smuggling; and/or, those that demonstrate, through act or omission knowledge or linkages to individuals or criminal groups that have or may have committed serious transnational crimes i.e. human smuggling.

v) Human Trafficking (IRPA Section 118)

Illicit migration scenarios identifying 'human trafficking' risks must be designed using intelligence analysis that identifies foreign nationals and/or Canadians who may be victims, or organizers of human trafficking related activities. The legislative authority related to human trafficking is included in section 118 of IRPA as well as multiple other legislative authorities found in the *Criminal Code of Canada*. The various laws application can respond to trafficking including kidnapping, forcible confinement, aggravated sexual assault, extortion, organized crime and prostitution-related offences.

Illicit migration scenarios must focus on those that have or may have committed an offence linked to human trafficking; and/or, those that demonstrate, through act or omission knowledge or linkages to individuals or criminal groups that have or may have committed serious transnational crimes i.e. human trafficking.

Scenario Creation and Review

The National Targeting Centre (TI, TT and TRIS) all review and track each step in the scenario development process including activations and modifications to ensure that prior to activation, scenarios meet CBSA policies and procedures including API/PNR legislative and regulatory use requirements, and do not have a negative impact on privacy, human rights and civil liberties.

Prior to activation, the scenario is impacted for volumetrics through the Targeting Data Analytics (TDA) unit and reviewed by Targeting Travellers (TT) for operational impacts and implementation with the objective to minimize traveller impacts. The Targeting Program Unit (TPU) will be provided with the scenario at the same time as TT and will conduct a review (Appendix A: Scenario Review Process), without impeding the scenario activation process, to ensure adherence to the appropriate statutory/regulatory requirements. If it is determined that a scenario possibly infringes upon the civil liberties, privacy or human rights of a traveller, TI will be immediately notified to discuss resolution. A communication protocol is further outlined in Appendix A.

The proposal is reviewed by the Targeting Rules, Indicators and Scenarios (TRIS) unit to ensure the scenario can be coded and activated in PAXIS. Once a scenario is activated, TRIS utilizes a rigorous monitoring and maintenance framework through which performance is reviewed and documented.

SBT Governance

The governance surrounding SBT leverages the existing targeting organizational framework to ensure it is effectively and efficiently managed and complies with international agreements, legislative and regulatory requirements.

Scenario Management Committee (SMC)

This Committee is responsible for making recommendations by conducting ongoing reviews of scenarios, scenario development, and management procedures to ensure scenario effectiveness, procedural efficiency, consistency and integrity. Scenarios viewed as ineffective, or not fulfilling program requirements may be deactivated or modified, and procedures will be

updated as required. In addition, the Committee investigates and reports on issues that impact the SBT process. The SMC is also responsible for reporting to the TPMC.

For further information, refer to the Terms of Reference (TR) of the SMC (Appendix B).

Targeting Program Management Committee (TPMC)

The mandate of this Committee is to ensure the management of the Targeting Program, including SBT, is efficient and effective, as well as operationally compliant with international agreements, legislative and regulatory requirements. In order to achieve this, the TPMC leverages the existing organizational framework and ensures the necessary leadership, communication and processes are in place.

For further information, refer to the TR of the TPMC (Appendix C).

Roles and Accountabilities

Operations Branch, National Border Operations Centre (NBOC), NTC

The NTC is responsible for the operational development and delivery of SBT, thereby making it accountable for the following:

- Ensuring adherence to all privacy, legislative, regulatory and policy requirements including written collaborative agreements, treaties and memoranda of understanding;
- Evaluating each scenario prior to activation to ensure compliance with all privacy, legislative and regulatory requirements;
- Developing and maintaining SBT operational procedures including scenario development, activation, monitoring and deactivation;
- Analyzing intelligence, reviewing examination and enforcement results, including the risk environment, trends and patterns to develop, modify or deactivate scenarios;
- Ensuring scenarios are operationally manageable and proportionate by assessing the operational impacts prior to activation;
- Collaborating with stakeholders in the scenario creation process;
- Recording and storing all intelligence and information used to develop a scenario in addition to maintaining the scenario development tracking log and scenario master list;
- Retaining all targeting scenario proposal templates in addition to recording the activation, modification and deactivation of scenarios;
- Identifying and monitoring API/PNR data quality and consulting with internal partners regarding data provision issues that impact the effectiveness of scenarios or the efficiency of PAXIS;
- Developing and distributing SBT performance reports to internal stakeholders;

- Assuming the responsibility for the scenario lifecycle including scenario development, activation, modification, and deactivation;
- Utilizing and maintaining a detailed log to provide an auditable record of scenario legislative and regulatory compliance review; and
- Coordinating meetings and maintaining records of the SMC.

Programs Branch, Enforcement and Intelligence Programs Directorate, Targeting Program Unit

The Targeting Program Unit is the functional authority for the targeting program, and is responsible for providing program strategy and policy direction related to SBT. Its accountabilities include:

- Providing strategic and functional direction to Operations Branch, and program policy, privacy, legislative and regulatory guidance to senior management concerning scenario-based targeting;
- Maintaining the *Scenario-Based Targeting Governance Framework*;
- Evaluating each scenario to ensure compliance with all privacy, legislative and regulatory requirements (for more information, refer to Appendix A "Scenario Review Process");
- Coordinating meetings and maintaining records of the Targeting Program Management Committee;
- Discussing SBT related issues with the Operations Branch, NBOC;
- Reporting and escalating issues on SBT-related matters, including program and policy matters and systems issues as required; and
- Supporting the NTC to evaluate systems, tools, business and process improvements facilitating operational delivery and ongoing enhancement of SBT (i.e. new systems/applications, analytical tools systems improvements and processes – e.g. PAXIS, SPSS modeller, and data warehouse).

Programs Branch, Traveller Programs Directorate, Air Programs Unit

The Air Programs Unit develops, amends, and maintains legislation and regulations related to traveller processing in the air mode and is the Office of Primary Interest for the API/PNR Program and PAXIS. Its accountabilities include:

- Providing program strategy and policy direction related to the collection and use of API/PNR;

- Developing and maintaining related high-level policies, regulations, and legislation for the acquisition and use of API and PNR data;
- Controlling and approving requests for access to PAXIS;
- Coordinating targeting and API/PNR systems changes/fixes or projects in conjunction with the Business Systems Integration Division; and
- Co-chairing (with the Targeting Program unit) the API/PNR Program and Targeting Program bi-weekly meetings where issues related to the API/PNR and Targeting Programs are identified, discussed, tracked and resolved.

Issue Escalation Process

1. Issues are first discussed between the Programs and Operations Branches' subject matter experts (SMEs).
2. If initial concerns raised between the SMEs are not resolved, the issue(s) are then brought to the SMC for a collective discussion and dispute resolution.
3. If the initial concerns that were raised during the SMC meeting are not resolved, the issue(s) are raised to the TPMC
4. If the initial concerns raised at TPMC are not resolved, the issue(s) are raised to the Enforcement and Intelligence Program Management Table (E&I PMT), the Traveller PMT or both, as required.

Note: any discussion between Programs and Operations on specific scenario issues are to be retained in the Operations' scenario folder.

The Chair and Deputy Chair of the E&I PMT (see Appendix D for the Terms of Reference) are accountable for providing guidance and direction to the responsible Directors as follows:

- Ensuring strategic planning and horizontal communications with regards to SBT.
- Providing guidance on implementing and monitoring performance measures.
- Identifying and leveraging best practices for SBT.
- Reviewing program costs and identifying opportunities for savings within SBT.
- Ensuring overall alignment with Agency priorities or long-term planning.

Appendix A: Scenario Review Process

Introduction

During the development of a scenario, the Canada Border Services Agency (CBSA) ensures that it does not contain any sensitive data, intrude on privacy, or violate civil liberties and human rights. The Agency will review each scenario prior to activation or modification in order to identify any potential impacts and to ensure compliance with current policy, legislation and regulations.

This appendix outlines the scenario components that are included in the review as well as the communication protocol for the National Targeting Centre (NTC) Operations and the Targeting Program authority.

Scenario Components

The National Targeting Centre (TI, TT and TRIS) review and track each step in the scenario development process including activations and modifications to ensure that prior to activation, all scenarios meet CBSA policies and procedures including API/PNR legislative and regulatory use requirements, and do not have a negative impact on privacy, human rights and civil liberties.

The Targeting Program unit (TPU) is responsible for the review of the scenario components prior to the activation or modification of a scenario to ensure adherence to CBSA policy, statutory and regulatory requirements. Should the TPU not complete the review prior to activation, the scenario will be activated in 'provisional' status until such time as the review is completed. The provisional status will permit operations, under time sensitive and exigent circumstances, to proceed with activation but track the scenario until such time as the Program review is complete.

The following scenario components will be reviewed by TPU:

1. Scenario Template
2. Scenario Description

1) Scenario Template

The scenario template must encompass the appropriate statutory requirements according to the applicable risk.

The *Customs Act* and *IRPA* are the primary legislative authorities that allow the CBSA to identify risks for the three categories of Contraband, Illicit Migration and National Security.

- Ensure the appropriate legislative authority (i.e. *Customs Act* or *IRPA)*, accurately reflects the identified risk category for terrorism or serious transnational crime.

2) Scenario Description

The scenario description includes the results of the trend analysis to support the scenario and the specific risk(s) for terrorism offences or serious transnational crimes meant to be captured by the scenario.

- Ensure the scenario description meets the regulatory requirements by not infringing on a person's privacy, civil liberties and human rights.

Communication Protocol

Following the intelligence analysis to develop the scenario and upon receipt of the operational volume impacts, Targeting Intelligence provides the draft scenario template to TT and TPU.

TT will review the draft scenario template for operational impacts and will advise TI upon approval.

TPU will review the draft scenario template, without impeding the scenario activation process, to ensure adherence to the appropriate statutory/regulatory requirements. If the scenario template and/or description does not meet the appropriate statutory/regulatory requirements, TPU will contact TI for further consultation.

TI provides TRIS with the TT-approved scenario template for activation. Once the scenario elements and description have been finalized, TRIS will provide TPU with the finalized version of the scenario template just prior to activation.

If the scenario template and/or description does not meet the appropriate statutory/regulatory requirements, TPU will contact TI and TRIS for further consultation to either deactivate or modify the scenario.

Should there be differing interpretations of the statutory/regulatory requirements, the concern will be raised at the next monthly Scenario Management Committee for resolution. If not resolved, the issue escalation process will be followed as detailed in the body of this framework document.

Appendix B: Terms of Reference – Scenario Management Committee

Context/Background

Scenario-Based Targeting (SBT) is a key part of the Canada Border Services Agency's (CBSA) pre-arrival traveller targeting program and supports the Agency's Risk Assessment Program by contributing to the identification and interception of suspected potential high and unknown risk people that may pose a threat to the national security, safety and prosperity of Canada. It also fulfils a commitment made by the CBSA under the Beyond the Border Action Plan to implement an enhanced SBT targeting methodology similar to that of the United States Customs and Border Protection.

Increasing targeting work volumes, finite resources, ongoing scrutiny of standardized/automated risk assessment and border security approaches and ever-changing risks/threats, necessitate ongoing robust rigour and scrutiny of the CBSA's risk management and assessment tools such as pre-arrival targeting's SBT process. In order to ensure the integrity and effectiveness of SBT and the overall success of the CBSA's traveller targeting program, the effectiveness of scenarios and the efficiency and integrity of their development and management processes/procedures, needs to be regularly reviewed and adjustments made as required.

Mandate/Expected Outcome

To ensure scenario based targeting is effective and complies with privacy, legislative and regulatory requirements.

Membership

Chair: NTC TRIS Manager
Co-Chair: NTC TI Manager
Secretariat: Targeting Rules Indicators and Scenarios (TRIS)

Representatives

- NTC – Targeting Intelligence (TI)
- NTC – Targeting Traveller (TT)
- NTC – Targeting Rules, Indicators and Scenarios (TRIS)
- NTC – Targeting Data Analytics (TDA)
- Targeting Program Unit
- Air Programs

* Note[1]: Other areas may be invited to attend meetings on an ad-hoc basis dependent upon specific agenda items.

* Note[2]: Members require Secret clearance and a working knowledge of SBT.

Meeting Frequency

Monthly

Members Roles and Responsibilities

- identify and discuss issues impacting scenarios (ex: data quality provision, review rates, scenario capacity limit, and elements for coding);
- provide recommendations for resolution;
- request additional information from Subject Matter Experts on scenarios;
- discuss and recommend scenarios for a possible scenario effectiveness assessment (SEA);
- review the outcome of the SEA; and
- Receive timely updates of legislative, regulatory, initiatives, systems, international or national agreements impacting SBT from Program authority.
- Review and make amendments to scenario development and processes and procedures, as required;
- Raising of issues to the Targeting Program Management Committee (TPMC) in accordance with the issues escalation process.

Meeting Organization

- A program officer from TRIS will act as the committee secretariat.
- Working group meetings will be held once a month; may be held more often as required.
- A report on the month's scenario activations, modifications and deactivations will be prepared by TRIS for discussion at the meeting.
- Records of discussion will be drafted and shared by the committee secretariat.

Appendix C: Terms of Reference – Targeting Program Management Committee

Mandate

To ensure the management of the Targeting Program is efficient and effective, as well as operationally compliant with international agreements, legislative and regulatory requirements. In order to achieve this, the Targeting Program Management Committee (TPMC) will leverage the existing organizational framework and will strive to have the necessary leadership, communications and processes in place.

Membership

Chairs:
Director of Intelligence, Targeting and Criminal Investigations Programs Management Division
and

Director of the National Targeting Centre

Note: The Director of Program Compliance and Outreach, Commercial Programs, will be an additional co-chair for TPMC-commercial meetings only

Secretary:
Targeting Program Unit

Members:
To include Managers and/or their representatives from the following areas:
Operations Branch:

- Commercial Operations Division
- National Targeting Centre
- Intelligence Operations and Analysis Division
- Traveller Operations Division

Programs Branch:

- Commercial Program and Policy Management Division
- Intelligence, Targeting and Criminal Investigations Programs Management Division
- Traveller Program and Policy Management Division

Note: Other areas may be invited to attend meetings on an ad-hoc basis dependent upon specific agenda items (i.e. IT or BSID).

Authority

The co-chairs of the committee have the authority to set the overall strategic direction of the Committee, to approve Committee agendas, and to request items be brought forward at a specified date.

The co-chairs retain the decision-making authority as to when to escalate items put before the committee if consensus cannot be achieved; however, the co-chairs shall seek to build consensus among members in carrying out this duty.

Roles and Responsibilities

To fulfill its mandate, the committee will:

- Receive a briefing from the Scenario Management Committee (SMC) meetings (for TPMC-traveller meetings only).
- Receive a briefing from the Commercial Risk Capability Management Committee (CRCMC) Committee meetings (for TPMC-commercial meetings only).
- Review and discuss targeting performance measurement, budget planning and accountability requirements.
- Identify and discuss data quality issues and industry data submission compliance rates.
- Identify and discuss effectiveness of national and regional intelligence in support of the National Targeting Model.
- Develop, review or recommend targeting policy, procedures, guidelines, processes and system requirements.
- Identify, analyze and propose solutions for any issues that have an impact on the delivery of the Targeting Program such as system issues and limitations, human resource planning, recruitment processes and training.
- Identify, analyze and propose solutions for any issues that have a direct impact on the success of the Targeting Program, such as the essential "inputs" (National, Regional, Internal Intelligence, data (internal, external), Exam Results (closing the loop), Partnerships (GC, International), as identified in the Internal Audit and Program Evaluation.

Meeting Frequency:

Separate committees will be held for commercial and travellers streams each month. It is anticipated there will be a joint commercial-travellers TPMC held two times a year to discuss cross-cutting issues in a consolidated forum.

Record of Discussion and Decision:

The secretariat of the committee is responsible for drafting and disseminating a Record of Discussion and Decision (RDD) to all attendees after a meeting is held.

Escalation:

The co-chairs are responsible for escalating, to the appropriate parties, any issues emanating from the meeting after an issue is identified.

Proxies to meetings:

Members of the committee shall nominate a proxy to attend a meeting if the member is unable to attend. Proxies are expected to brief all affected parties within their Unit, Division and Directorate on all decisions made at the committee.

Please note that membership is recommended to be at the manager and senior advisor level. Proxies should be first at the senior advisor level and if neither the manager nor senior advisor is available, a senior program officer can represent their area.

Quorum Requirements:

A minimum of four (4) committee members is required for the meeting to be recognized as an authorized meeting. If either of the co-chairs or their representatives is unavailable, the scheduled meeting may be cancelled or rescheduled.

Appendix D: Terms of Reference – Enforcement and Intelligence Program Management Table

Mandate

The Enforcement and Intelligence Program Management Table (EI PMT) members will consult jointly and provide integrated and functional guidance to the following eight (8) EI programs: Intelligence, Targeting, Security Screening, Criminal Investigations, Immigration Investigations, Detentions, Hearings and Removals. The Intelligence Program also includes some areas under International Region and the National Targeting Centre.

This PMT is a focussed, action-oriented decision making body and is responsible for providing leadership on the EI's program strategic policy direction, priority setting, performance measurement, risk identification and mitigation strategies, workforce training and leaning requirements and making financial recommendations.

Membership

Chair	• Director General, Enforcement and Intelligence Programs Directorate, Programs Branch
Deputy Chair	• Director General, Enforcement and Intelligence Operations Directorate, Operations Branch
Secretariat	• Director, Program Performance, Reporting and Transformation Division, Enforcement and Intelligence Programs Directorate, Programs Branch
Standing Members	• Executive Director, Enforcement & Intelligence Programs, Programs Branch • Director General, Global Border Management and Data Analytics, Programs Branch • Director General, National Border Operations Centre, Operations Branch • Director General, International Operations, Operations Branch • Executive Director, Pacific Region, Operations Branch • Director General, Training & Learning, Human Resources Branch • Director General, Corporate Governance & Accountability, Corporate Affairs Branch • Director General, Resource Management Directorate, Comptrollership Branch • Director, National Targeting Centre, Operations Branch • Director General, Transformation and Oversight, Comptrollership Branch

	• Director General, Enterprise Architecture/Information Management, IST Branch • Directors, Enforcement and Intelligence Programs, Programs Branch • Senior Advisor, Programs & Operations Communications, Communications Directorate, Corporate Affairs Branch
Ad Hoc Members	• Directors, Enforcement and Intelligence Operations, Operations Branch **Based on the agenda items, attendance to the PMT will vary for Ad Hoc Members**

Note: Each Standing Member of the EI PMT shall nominate one proxy at the Director level to attend meetings in the event that the Member is unable to attend. Every effort should be made by each Standing Member to attend all meetings. Every effort should also be made to ensure that a proxy is available for all meetings that the Standing Member is unable to attend, and is well briefed on the operations of the PMT. Subject matter experts and observers may be invited to attend a PMT meeting at the Chair's discretion.

Responsibilities and Duties

The EI PMT has the responsibility for decisions that affect the functional direction and oversight, budget management, and monitoring and performance reporting of the Enforcement and Intelligence Programs. To do this, the EI PMT will focus on the following areas:

1. Serve as an active and dynamic oversight body with regards to financial, budgetary, training and learning, and human resources planning issues, and provide input on the PMT's forward agenda.

2. Support vertical and horizontal communications and engagements and seek to build consensus among Standing Members and Ad Hoc Members.

3. Provide strategic direction for EI stakeholder engagement, including (a) form and dissolve EI level committees, and (b) establish reporting requirements for committees. These committees will then analyze/examine and propose resolutions and report back their findings to the EI PMT.

4. Ensure alignment of identified priorities and evaluate performance measurements on a quarterly basis.

5. Report to the President on the PMT progress on established performance indicators and make recommendations relating to Criminal Investigations, Immigration Enforcement Program Activities and Targeting, and the Intelligence and Security Screening Program Sub-Activities, in collaboration with the Program Policy Committee (PPC) and Executive Committee (EC).

6. Provide direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

Chair

The duties of the Chair of the EI PMT are an extension of his or her organizational responsibilities as the DG of the Enforcement and Intelligence Programs Directorate.

1. Serve as the single point of accountability for the PMT, as well as the decision-making authority on items put before the PMT.

2. Retain the sole authority to make a decision to escalate issues to the Program Policy Committee (PPC) for consideration, resolution, and/or guidance.

3. Responsible for vertical and horizontal communications and engagement.

4. Establish a results measurement framework for monitoring the PMT's performance, while evaluating progress on a quarterly and annual basis.

5. Facilitate meaningful and effective meetings, ensuring that items brought to the PMT have been broadly and adequately consulted.

6. Determine PMT membership in collaboration with the Deputy Chair.

7. Responsible for providing direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

8. Delegate duties and oversight of certain areas of responsibility to the Deputy Chair.

Deputy Chair

1. Assume the roles and responsibilities of the Chair in the Chair's absence, as well as other duties and responsibilities as assigned by the Chair.

2. Collaborate with the Chair in determining PMT membership.

3. Build consensus with the Chair, on key issues and decision points before and after PMT meetings, to address contentious issues, potential conflicts of interest and work towards integrating program and operational activities to achieve the best results possible.

4. Consult with senior management in the Regions and represent their views to the extent possible at EI PMT meetings, while reporting back to them on all PMT business.

Governance Structure

The EI PMT is accountable to the Program Policy Committee (PPC). The role of the PPC is to advise Executive Committee (EC) on strategic policy and ensure the ongoing development of CBSA policy and program delivery and to identify and manage functional management issues in relation to risk.

The PMT is the governing authority for director-level committees and managerial program committees. Director level committees are:

- National Inland Enforcement Committee,
- National Intelligence, Targeting and Security Screening Committees, and
- National Criminal Investigations Committee.

Committee membership is composed of both Headquarters and regional members.

Managerial working level groups should exist for all EI Programs. Managerial level working group membership is composed of the program's respective national managers and regional managers.

It is expected that issues will be brought forward at the appropriate working level and follow the governance hierarchy in seeking approvals by, or providing briefings to, the relevant decision-making body. Director level committees may additionally wish to seek approval or consult with the EIOD Directors/DG Operations Committee on relevant issues.

The committees and working groups meet on a regularly scheduled basis and report to the PMT quarterly on issues such as risk/risk mitigation, performance and financial management.

Please see the Annex for further details on the EI PMT Governance structure.

Table Operation

Frequency and Duration

The EI PMT shall meet on a three week schedule on Wednesdays, or more frequently if required. *Ad hoc* meetings may be scheduled as required at the request of the Chair.

Quorum

A minimum of four EI PMT Standing Members, including the Chair or the Deputy Chair, are required for the meeting to be recognized as an authorized meeting.

Materials and Records of Discussion

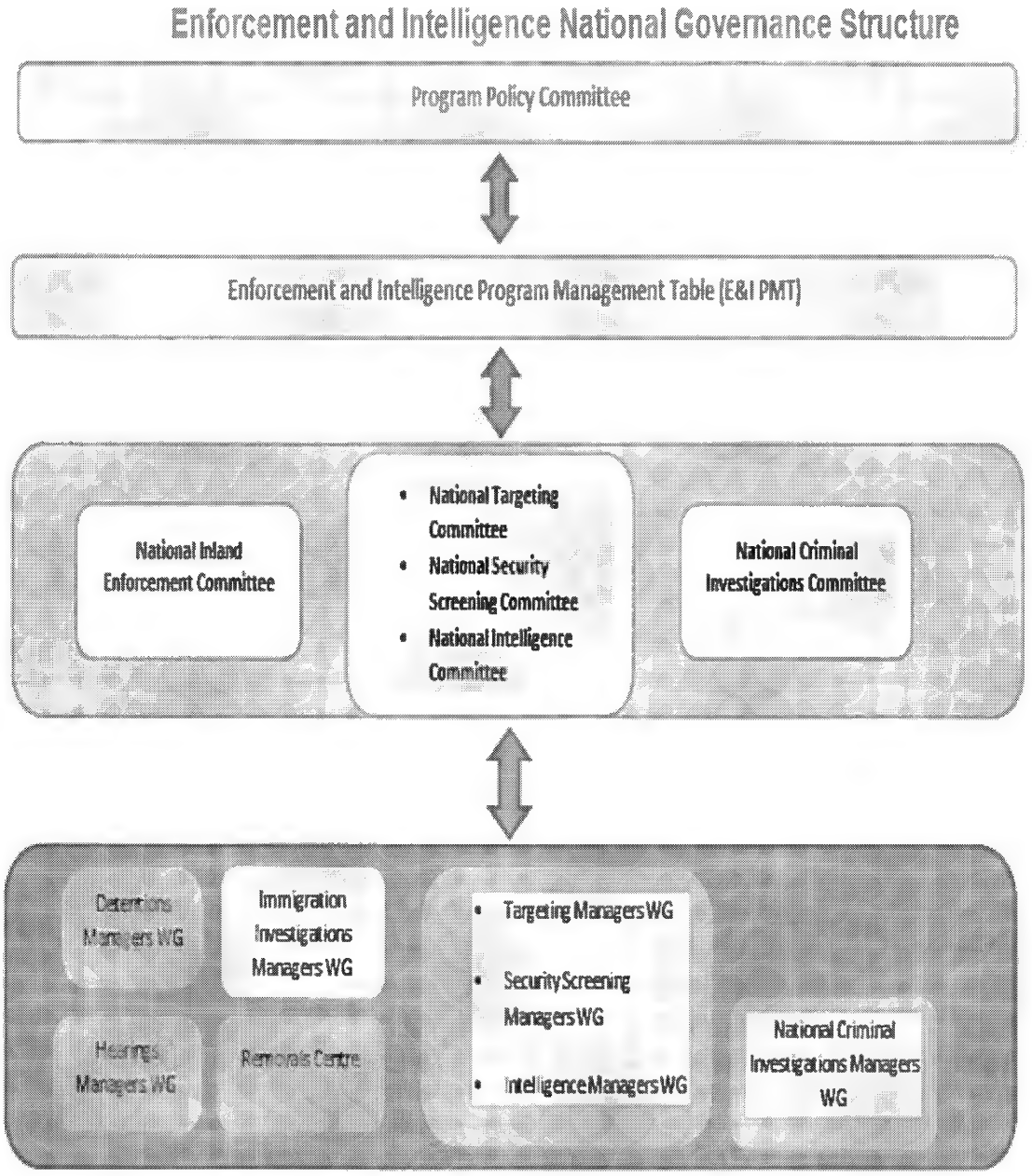
The EI PMT Secretariat will prepare the Agenda and the Record of Discussion (RoD) for each meeting and provide to the Chair for final review and approval. The RoD shall include clear action items, with assigned leads and Brought Forward (BF) dates. It will also include standing and forward agenda items. The Secretariat is responsible for disseminating the RoD to all Standing Members prior to the next meeting. RoDs and Annexes will be made available to EI PMT Members as needed in an effort to promote information sharing. The RoD and identified action items from each meeting will be maintained and monitored by the Secretariat.

The Chair shall finalize and approve the agenda for each EI PMT meeting one week before the scheduled meeting. Materials are normally available to EI PMT Members two business days in advance of any meetings.

Values Based Leadership and Organizational Culture

EI PMT Members, through their actions and words, shall demonstrate their commitment to the highest standards of integrity, ethical values and professionalism in the performance and functional management of programs.

Annex:



PROTECTED B

Air Passenger Targeting (APT)

Module 3: Air Passenger Targeting Process

January 2016

Participant's Guide

Training and Learning Directorate

The Targeting Policy Unit, Targeting Policies and Program Management Division, Canada Border Services Agency, developed this material in partnership with subject matter experts. The content was reviewed for technical accuracy in January 2016.

Examples and scenarios have been created using fictional names. Any resemblance to persons real, imaginary, or deceased is purely coincidental. There is no intention for examples to depict stereotyping on any basis.

Unless otherwise stated, whenever the masculine pronoun is used, both men and women are included.

Printed copies of this controlled document are considered UNCONTROLLED.

The Training and Learning Directorate maintains the master version of this document.

Table of Contents

Before you Begin

Introduction

By now, you should have a basic understanding of how the CBSA receives advanced passenger information and the legislation pertaining to its access, retention and protection. Moving forward, you need to know how this information can be used to make a decision as to whether or not to issue a target.

Relevance

As a targeting officer, you are required to analyze and leverage various pieces of information received via API, DCS and PNR messages to identify risk indicators and confirm or the negate risk. It is important that you have a clear understanding of air passenger targeting process and methodologies to successfully determine the need to issue a target based on the information available to you.

Objective

After completing this lesson, you will be able to:

- Understand the air passenger targeting process and methodologies
- Use API, DCS and PNR data elements to identify risk indicators

Prerequisites

- Completion of the Foundations of Targeting Course.
- Completion of APT Module 1 and 2.

Competencies

- Information seeking techniques
- Judgment
- Deductive reasoning
- Critical thinking

Duration

Please note that these are estimates only.

Topic	Time
Air Passenger Targeting Process	7h 30m
Total	**7h 30m**

Overview

When API/PNR messages are received by the CBSA, they are processed and made available to targeting officers via PAXIS, the primary air targeting application, which is part of the CBSA Integrated Customs System (ICS). PAXIS provides targeting officers various workflows that will assist them with the following targeting methodologies:

- Scenario Based Targeting
- Flight List Targeting ("sort and assess").

In this module, you will learn about both targeting methodologies, and how to identify risk indicators within the information provided to you.

1. Scenario Based Targeting

Background

The CBSA
follow a similar methodology to conduct targeting of unknown high risk travellers.

In 2014, technological changes were made to PAXIS that allows CBSA to create scenarios for use in identifying suspected high risk travellers. These capabilities allow the CBSA to:

- react in real time to ever changing trends and risks
- respond effectively to national and international incidents
- effectively work in partnership with other international Customs and Immigration partners who also utilize scenario based targeting methodologies.

These capabilities ensure that common risks among partners can be quickly identified and actioned. These capabilities also ensure that the CBSA can target specific risks and threats. The scenarios allow for the immediate identification of travellers matching data elements which are known to be associated with threats to national security, illicit migration, contraband and other national priorities. This

process allows targeting officers to conduct further analysis and review in a timely fashion. This in turn enables the interception of high risk individuals upon arrival in Canada.

What Is a Scenario?

A scenario is a grouping of elements which are indicative of an identified risk trend or pattern.

Scenarios are identified by a risk category. The current categories that are targeted within PAXIS include national security, contraband, immigration and other. Scenarios can be specific to risks that are local, regional and/or national in nature. Scenarios can also be implemented in support of projects/Joint Forces Operations (JFO) initiatives.

How is a Scenario Created?

Scenarios are developed based on information from a variety of sources including but not limited to:

Types of information that contribute to scenarios include:

When a risk trend is identified or intelligence is received, the information is passed by the person, unit or organization identifying the trend, to the Targeting Intelligence (TI) unit at the NTC as a recommendation to implement a scenario and if necessary conduct additional analysis.

Furthermore, Data Analytics Unit (DAU) at the NTC will perform preliminary volumetric tests to identify the potential impact of the scenario on both Targeting and Port of Entry Operations. If the submission is considered complete and the impacts seem reasonable, the scenario recommendation is forwarded to scenario administrators and is created in the PAXIS Rules Engine. The process of building the scenario in the rules engine can, if necessary, be completed in a relatively short time frame and can be activated whenever the CBSA deems appropriate (immediately or later).

What is a Scenario Match?

If the risk is determined to be valid, a target will be issued from PAXIS or within ICES which will enable the interception of the traveller for further processing upon arrival in Canada.

2. Flight List Targeting

Flight List targeting methodology requires targeting officers to perform research and analysis on Canada bound flights arriving in regions assigned to them.

If the risk cannot be negated, targeting officers will issue a target in PAXIS and/or ICES.

Comprehensive Review consists of detailed research and analysis of identified high risk travellers. It may include following steps as determined by a targeting officer:

1.
2.
3.
4.
5.

3. Lookout List / RFI

Lookout List

Request for Information (RFI)

Occasionally, targeting officers will be asked for additional verification of information on select travellers

4. Targeting Support Systems Overview

As a Targeting officer, you will be using multiple internal and external databases when performing your duties. You will receive an in-depth training on all the targeting support systems later on. In this module, however, you will receive a high-level introduction to most commonly used systems.

Integrated Customs System (ICS)

ICS is a CBSA suite of applications that includes access to Integrated Primary Inspection Line (IPIL), Passage History and Secondary

Processing, PAXIS and Integrated Border Query (IBQ). ICS also grants access to other applications such as Global Enrolment (NEXUS).

ICS Passage History (PH)

PAXIS

Paxis provides targeting officers with all the workflows available to assist them with both scenario based and flight list targeting methodologies. These workflows and other features of PAXIS will be covered in PAXIS-only training later on.

All target decisions and follow-up activities, regardless if a review was conducted based on a traveller with a scenario match or not, are recorded in PAXIS.

Integrated Customs Enforcement System (ICES)

The ICES database contains all seizures, lookouts, export control activities, search and arrest activities, and selected immigration records. ICES also includes information on travellers and vehicles passage history.

Global Case Management System (GCMS)

GCMS is CIC's single, integrated and world-wide system used to process applications for citizenship and immigration services. Used as part of the comprehensive review by targeting officers to verify immigration status of a traveller.

Secure Tracking System (STS)

The primary role of STS is to screen Temporary and Permanent resident visa applications. STS contains information on individuals involved in and/or associated with organizations involved in war crimes, crimes against humanity and/or terrorist activities, organized crime, money laundering, terrorist financing and people smuggling.

INTERPOL

INTERPOL gives the CBSA immediate access to a range of information on internationally known criminals such as: wanted international fugitives or persons of interest and Stolen/Lost Travel Documents. A majority of this type of information is communicated through Interpol Notices.

Open Source

Information collected from publically available sources such as social media, blogs, news publications, government databases, and forums.

Intelligence Management System (IMS)

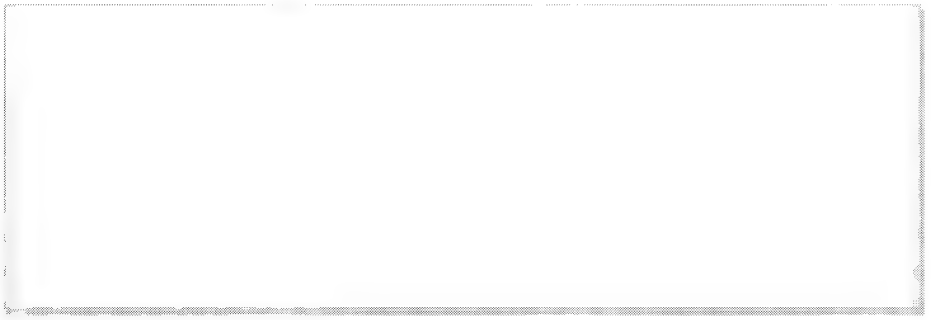
Integrated Border Query (IBQ)

The system does not perform analysis of the data, it only presents it.

5. Risk Indicators

The API/DCS and PNR elements are used to establish a multiplicity of indicators.

If a multiplicity of indicators is gathered and they have not been negated, a target should be issued for that passenger.



Data Elements

There are over 400 individual pieces of information about a traveller that CBSA can receive via API/DCS and PNR messages. Within all that information, there are a number of possible indicators which can be used for targeting purposes.

In this section, you will learn how to use the data elements available to you as a targeting officer, and how to identify risk indicators within that information.

5.1 Summary

Date of Birth

Questions relating to the date of birth:

Gender

Questions relating to the gender:

Employee

This indicates if the passenger is an employee of the carrier on which they are flying.

Locator

The locator is a unique 6 digit alpha-numeric number assigned to a booking; the file number of the PNR.

Question regarding locator number:

in Group

This is the count of passengers included in the reservation that the current passenger is part of.

Frequent Flyer

Frequent flyer information such as the travel program number as well as the sponsor of the program i.e. Air Canada or Aeroplan, can be found in the Frequent Flyer section of traveller details.

Travel Agency Info

In the Travel Agency area of Traveller details, is information including Travel Agency Name and Travel Agency IATA number (This is an 8 digit International Air Transport Association (IATA) number for the travel agency where the ticket was booked.)

The Travel Agency info also contains the Profile City, Terminal City, and Agent of the travel agency used to create the reservation.

Questions regarding the Travel Agency Info:

Ticket Issued City

IATA Airport Code representing the closest airport where the ticket was issued.

Lead Time

Questions relating to lead:

Date Booked

The date that the reservation was made.

Departure Date

The departure date of the first segment in the reservation.

Note: *Dates are used for automated calculation of the lead time by the system*

Link Status

The link status is the quality of the linkage between the PNR and the API. Here are the possible results you may see on your screen for link status:

Ticket Type

The check-in ticket type (e.g., manual (handwritten, electronic (paperless, or automatic (printed)). E-ticket indicators are also available.

5.2 DCS (Check-In) / Seat / Luggage

The DCS portion of the Traveller Details is specific to the selected passenger and contains information related to check-in.

Sequence

The sequence is the order in which passengers check in for this segment of the flight.

Time

The time the passenger checked in at the airport for this segment of the trip.

Seat

Seat assigned to a passenger at time of check-in. Some passengers pre-select their seat assignments when they make their bookings. However, many seats are assigned during the check-in process.

Questions relating to seat #:

Classes/Cabin Fare

This column contains the passenger's booked cabin class. This is an indication of where they sat on the plane (e.g., first class, coach, etc.) See Appendix A for an explanation of all the possible class codes.

Questions relating to classes/cabin fares:

Checked Bags

Checked Bags is the number of bags checked in by the passenger.

Questions regarding checked bags:

Baggage weight

Questions regarding baggage weight:

Pool

This is a number assigned to a passenger's bags when they check in as part of a group.

Questions you can ask yourself:

Group Code/Group Name

This is the code assigned to the group the passenger is part of.

Tag Details

Handler

This field may contain the two-digit IATA code of the carrier that issued the tag and that is transporting the bags. It may also indicate a personal identifier specific to a handler employed by that carrier. See **Appendix B** for the list of IATA codes.

Number

The individual bag tag number.

Destination

The three-character IATA airport code indicating the final destination for this bag (e.g., YUL = Montreal – Pierre Elliott Trudeau International Airport).

Question you can ask yourself:

Type

The bag's type as defined by the bag tag. This data element can contain the following values:

- Unknown
- Local
- Transit
- Cancelled
- Manual
- Extra
- Reissued
- Limited release
- Animal in hold

5.3 Itinerary

The "Itinerary" section contains a chronological view of the passenger's trip and the places they departed, visited or transited. It displays the different segments of travel, containing their arrival and departure points, flight numbers, dates and times of departures and arrivals, as well as cancelled flights.

Departure/Arrival Airports

The airports are identified by a three-character airport code (e.g., YOW = Ottawa International Airport). The departure/arrival airports are representative of that segment of the flight.

Questions relating to departure/arrival airports:

Departure Date

This is the date of departure this segment of the trip.

Questions relating to departure date:

Open/ARNK

A sub-identifier for the current segment line. The possible values are "Open" – this indicates that there is no specified return date for the

passenger – or "ARNK" – this indicates that there is an unidentified portion of the routing

Cancelled Reservation

This section identifies the number of cancelled segments and the dates associated with each segment that was cancelled.

Changes and alterations to a passenger's itinerary can be made for a variety of personal reasons. Changes made between the dates of booking and prior to the first segment of travel are less of a concern. They can be attributed to last minute adjustments.

Questions relating to cancelled reservation:

5.4 Traveller

This section contains specific passenger information retrieved from API, DCS and PNR messages received. the following information may be of interest:

Nationality

This is the nationality provided by the passenger's documentation or as declared by a passenger when checking in or reserving a ticket.

Questions relating to nationality:

Documents

All document provided in API, DCS and PNR messages will display in this area. It will identify the doc types, the doc origin, the country where the document was issued, the date of issue, the date of expiry, and what type of message within PAXIS this document is found (API, DCS or PNR)

Questions relating to document 1 and 2:

Type

This is the type of document presented by the passenger.

Questions relating to type:

Origin

This is the country of origin of the document presented by the passenger. Most international air passengers are either travelling to or from their country of residence.

Questions regarding origin:

Name(s)

The passenger's name as recorded at the time of the reservation. It may contain the name(s) of the other passengers with whom this passenger is travelling.

Questions regarding reservation names:

PNR Name Changes

Displays whether the passenger's name has been changed from the original reservation and when the changes were made.

Questions relating to reservation name changes:

5.5 Address(es)

This section includes the collection of all address information provided at time of booking.

Type

The travel agency or airline usually requests this information so that they can contact the passenger if there are changes or updates to their reservation.

Questions relating address:

5.6 Telephone #(s)

This is a collection of all telephone information at the time of booking.

Type, Number, City

The possible values of these elements are: unknown, home phone number, business agent's phone, FAX number, emergency number, e-mail format within phone field, address field format within phone field, Person Will Call (PWC), unrecognized type, no contact given or mobile phone number, and the city.

Questions about phone number:

5.7 Payments

This is a collection of all payment information including credit cards, found within the PNR. The format of the credit card information is as follows:

Type

The type of credit card used. The possible values of this element are: American Express, MasterCard, Visa, Discover, Other and Diners Club.

Number

The actual credit card number that was used to pay for the flight. Only the last 4 digits of the credit card number are available to the CBSA.

Credit Card Owner

5.8 Ticket

This section contains all ticket information found within the PNR and DCS.

Locator No.

This is the unique file number created at the beginning of the booking. This number does not change even if flights are cancelled or changed.

Ticket No.

This is the passenger's ticket number.

Question regarding ticket number:

Amount of Payment

This identifies the total cost of the ticket, and displays the currency used for payment.

Form of Payment

This identifies how the passenger paid for the airfare. The possible values are: unknown, cash, cheque, frequent flyer ticket, government travel request, credit card or exchange ticket.

Questions regarding form of payment:

5.9 Frequent Flyer

This section contains all available frequent flyer information found within PNR and DCS.

This data element contains the frequent flyer card holder's name that is found in the DCS.

Questions regarding frequent flyer.

Conclusion

As a targeting officer, you are required to analyze and leverage various data elements of the API, DCS and PNR messages to identify risk indicators and confirm or the negate risk. During a comprehensive review, the data elements available to you will help you identify risk indicators for the flight list targeting, and add to the indicators already found in the scenario based targeting mode. Finally, the API, DCS and PNR data elements will assist you in making a target/no target decision.

Commonly Used Acronyms

API – Advanced Passenger Information

CAIPS – Computer Automated Immigration Processing System

CBRNE – Chemical, Biological, Radiation, Nuclear, Explosives

CBSA – Canada Border Services Agency

CFRO – Canada Firearms Registry Office

CPIC – Canadian Police Information Centre

CSIS – Canadian Security Intelligence Service

CSQ – Client Status Query

IBQ – Integrated Border Query

ICES – Integrated Customs Enforcement System

ICS – Integrated Customs System

IMS – Intelligence Management System

FBI – Federal Bureau of Investigations

FOSS – Field Operations Support System

GCMS – Global Case Management System

MOU – Memorandum Of Understanding

NCMS – National Case Management System

NTC - National Targeting Centre

NCIC – National Crime Information Center

ORS – Occurrence Reporting System

PH – Passage History

PNR – Passenger Name Record

PAXIS – Passenger Information System

RAPID – Random Access Personal Information Data

RCMP – Royal Canadian Mounted Police

SBT – Scenario Based Targeting

TPU – Targeting Policy Unit

TPPMD – Targeting Policies and Programs Management Division

TRMS – Targeting Risk Management Strategy

USCBP – United States Customs and Border Protection

Airline Class Codes

First class codes

- F = Full-fare first class
- P = First class
- A = First class discounted
- R = First class suites (currently only Singapore Airlines and formerly Supersonic (Concorde)

*a lowercase "n" after any class code indicates night service

Business class codes

- C, J or D = Full-fare business class
- I or Z = Business class discounted

*a lowercase "n" after any class code indicates night service

Economy class codes

- B, H, K, L, M, N, Q or V = Economy/coach discounted
- E = Shuttle service (no reservation allowed) or economy/coach discounted
- G = Conditional reservation
- S or Y = Economy/coach
- T = Economy/coach discounted or premium
- U = Shuttle service (no reservation needed/seat guaranteed)
- W = Economy/coach premium

*a lowercase "n" after any class code indicates night service

On most airlines an unrestricted economy ticket is booked as a Y fare. Full fare tickets with restrictions on travel dates, refunds, or advance reservations are commonly classed as B, H, or M, although some airlines may use S, W, or others. Heavily discounted fares, commonly T or W, will not permit cabin upgrades, refunds, or reservation changes, may restrict frequent flyer program eligibility, and/or impose other restrictions. Other fare codes such as X are restricted for use by consolidators, group charters, or travel industry professionals.

Canada Border Services Agency | Agence des services frontaliers du Canada

Enforcement and Intelligence Program Management Table

Terms of Reference

Updated: October 2016

PROTECTION • SERVICE • INTEGRITY

Canada

ACCEPTANCE

These Terms of Reference represent a formal agreement and commitment by the Programs, Operations and Comptrollership Branches in the collaborative management of the Enforcement and Intelligence Program Management Table.

Authorization	
Lesley L. Soper Chair, Enforcement and Intelligence Program Management Table A/Director General, Enforcement and Intelligence Programs Directorate, Programs Branch	Date:
Andrew LeFrank Deputy Chair, Enforcement and Intelligence Program Management Table Director General, Enforcement and Intelligence Operations Directorate, Operations Branch	Date:

Membership

The Enforcement and Intelligence Program Management Table (EI PMT) members will consult jointly and provide integrated and functional guidance to the following eight (8) EI programs: Intelligence, Targeting, Security Screening, Criminal Investigations, Immigration Investigations, Detentions, Hearings and Removals. The Intelligence Program also includes some areas under International Region and the National Targeting Centre.

This PMT is a focussed, action-oriented decision making body and is responsible for providing leadership on the EI's program strategic policy direction, priority setting, performance measurement, risk identification and mitigation strategies, workforce training and learning requirements and making financial recommendations.

Membership

Chair	• Director General, Enforcement and Intelligence Programs Directorate, Programs Branch
Deputy Chair	• Director General, Enforcement and Intelligence Operations Directorate, Operations Branch
Secretariat	• Director, Program Performance, Reporting and Transformation Division, Enforcement and Intelligence Programs Directorate, Programs Branch
Standing Members	• Executive Director, Enforcement & Intelligence Programs, Programs Branch • Director General, Global Border Management and Data Analytics, Programs Branch • Director General, International Region, Operations Branch • Executive Director, Pacific Region, Operations Branch • Director General, Training and Development, Human Resources Branch • Director General, Corporate Planning and Reporting, Corporate Affairs Branch • Director General, Enterprise Architecture and Information Management, Information, Science and Technology Branch • Director General, National Border Operations Centre, Operations Branch • Director, National Targeting Centre, Operations Branch • Director, Strategic Finance and Costing, Comptrollership Branch • Directors, Enforcement and Intelligence Programs, Programs Branch
Required Participants	• Senior Advisor, Programs and Operations Communications, Corporate Affairs Branch • Manager, Strategic Finance and Costing, Comptrollership Branch • Senior Program Advisor, Governance and Financial Oversight Unit, Enforcement and Intelligence Programs, Programs Branch

Ad Hoc Members *	• Directors, Enforcement and Intelligence Operations, Operations Branch • Directors, International Region, Operations Branch • Directors, National Border Operations Centre, Operations Branch • Director, Business Systems Integration (E&I support), ISTB Branch **Based on the agenda items, attendance to the PMT will vary for Ad Hoc Members**

Note: Each Standing Member of the EI PMT shall nominate one proxy at the Director level to attend meetings in the event that the Member is unable to attend. Every effort should be made by each Standing Member to attend all meetings. Every effort should also be made to ensure that a proxy is available for all meetings that the Standing Member is unable to attend, and is well briefed on the operations of the PMT. Subject matter experts and observers may be invited to attend a PMT meeting at the Chair's discretion.

Responsibilities and Duties

The EI PMT has the responsibility for decisions that affect the functional direction and oversight, budget management, and monitoring and performance reporting of the Enforcement and Intelligence Programs. To do this, the EI PMT will focus on the following areas:

1. Serve as an active and dynamic oversight body with regards to financial, budgetary, training and learning, and human resource planning issues, and provide input on the PMT's forward agenda.

2. Support vertical and horizontal communications and engagements and seek to build consensus among Standing Members and Ad Hoc Members.

3. Provide strategic direction for EI stakeholder engagement, including (a) form and dissolve EI level committees, and (b) establish reporting requirements for committees. These committees will then analyze/examine and propose resolutions and report back their findings to the EI PMT.

4. Ensure alignment of identified priorities and evaluate performance measurements on a quarterly basis.

5. Report to the President on the PMT progress on established performance indicators and make recommendations relating to Criminal Investigations, Immigration Enforcement Program Activities and Targeting, and the Intelligence and Security Screening Program Sub-Activities, in collaboration with the Program Policy Committee (PPC) and Executive Committee (EC).

6. Provide direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

Chair

The duties of the Chair of the EI PMT are an extension of his or her organizational responsibilities as the DG of the Enforcement and Intelligence Programs Directorate.

1. Serve as the single point of accountability for the PMT, as well as the decision-making authority on items put before the PMT.

2. Retain the sole authority to make a decision to escalate issues to the Program Policy Committee (PPC) for consideration, resolution, and/or guidance.

3. Responsible for vertical and horizontal communications and engagement.

4. Establish a results measurement framework for monitoring the PMT's performance, while evaluating progress on a quarterly and annual basis.

5. Facilitate meaningful and effective meetings, ensuring that items brought to the PMT have been broadly and adequately consulted.

6. Determine PMT membership in collaboration with the Deputy Chair.

7. Responsible for providing direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

8. Delegate duties and oversight of certain areas of responsibility to the Deputy Chair.

Deputy Chair

1. Assume the roles and responsibilities of the Chair in the Chair's absence, as well as other duties and responsibilities as assigned by the Chair.

2. Collaborate with the Chair in determining PMT membership.

3. Build consensus with the Chair, on key issues and decision points before and after PMT meetings, to address contentious issues, potential conflicts of interest and work towards integrating program and operational activities to achieve the best results possible.

4. Consult with senior management in the Regions and represent their views to the extent possible at EI PMT meetings, while reporting back to them on all PMT business.

Governance Structure

The EI PMT is accountable to the Program Policy Committee (PPC). The role of the PPC is to advise Executive Committee (EC) on strategic policy and ensure the ongoing development of CBSA policy and program delivery and to identify and manage functional management issues in relation to risk.

The PMT is the governing authority for director-level committees and managerial program committees. Director level committees are:

- National Inland Enforcement Committee,
- National Intelligence, Targeting and Security Screening Committees, and
- National Criminal Investigations Committee.

Committee membership is composed of both Headquarters and regional members.

Managerial working level groups should exist for all EI Programs. Managerial level working group membership is composed of the program's respective national managers and regional managers.

It is expected that issues will be brought forward at the appropriate working level and follow the governance hierarchy in seeking approvals by, or providing briefings to, the relevant decision-making body. Director level committees may additionally wish to seek approval or consult with the EIOD Directors/DG Operations Committee on relevant issues.

The committees and working groups meet on a regularly scheduled basis and report to the PMT bi-annually on issues such as risk/risk mitigation, performance and financial management by undergoing a Program Health Check. The Program Health Check ensures regular governance oversight by the Table and provides an opportunity for program managers to seek guidance or socialize key program management or policy issues.

Please see Appendix A for further details on the EI PMT Governance structure and Program Health Check calendar.

Table Operation

Frequency and Duration

The EI PMT shall meet on a monthly schedule on Wednesdays, or more frequently if required. *Ad hoc* meetings may be scheduled as required at the request of the Chair.

Quorum

A minimum of four EI PMT Standing Members, including the Chair or the Deputy Chair, are required for the meeting to be recognized as an authorized meeting.

Materials and Records of Discussion

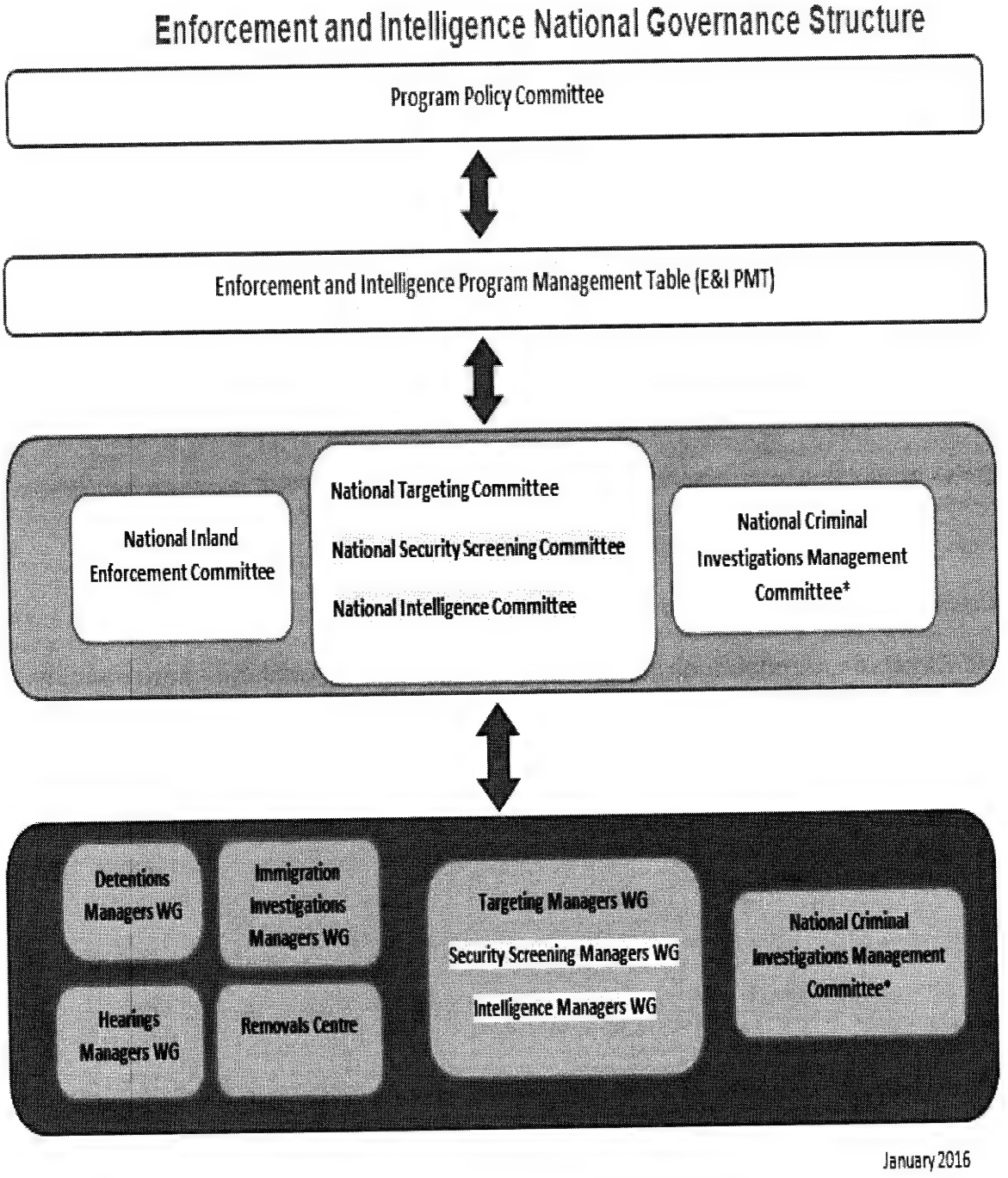
The EI PMT Secretariat will prepare the Agenda and the Record of Discussion (RoD) for each meeting and provide to the Chair for final review and approval. The RoD shall include clear action items, with assigned leads and Brought Forward (BF) dates. It will also include standing and forward agenda items. The Secretariat is responsible for disseminating the RoD to all Standing Members prior to the next meeting. RoDs and Annexes will be made available to EI PMT Members as needed in an effort to promote information sharing. The RoD and identified action items from each meeting will be maintained and monitored by the Secretariat.

The Chair shall finalize and approve the agenda for each EI PMT meeting one week before the scheduled meeting. Materials are normally available to EI PMT Members two business days in advance of any meetings.

Values Based Leadership and Organizational Culture

EI PMT Members, through their actions and words, shall demonstrate their commitment to the highest standards of integrity, ethical values and professionalism in the performance and functional management of programs.

Appendix A:



Yellow: in development ; * combined manager/director committee

President's Office Time Stamp / Timbre dateur du bureau du président

Canada Border Services Agency / Agence des services frontaliers du Canada

PROTECTED A / PROTÉGÉ A

CBSA/ASFC-14-04251

ROUTING SLIP/BORDEREAU D'ACHEMINEMENT

		ACTION REQUIRED/ MESURE REQUISE	
Name and Telephone Number/ Nom et numéro de téléphone	**Initials and date/ Initiales et date**	**Action**	**Information**
Vice-President/ Vice-président Richard Wex		☒	☐
Associate Vice-President/ Vice-président associé Peter Hill	25/3	☐	☒
Director General/ Directrice générale Monik Beauregard	20 March 2015		
Executive Director/ Directrice exécutive Lesley Soper	**Absent**		

Subject/Objet : **Update on the Governance and Oversight of Scenario Based Targeting (SBT)**
Action/Mesure : For Information
BF/AR : 2015-03-19

Attached is a briefing note to update you on the status of the Governance and Oversight of Scenario Based Targeting (SBT). We have also provided you with the SBT Policy and Governance document.

Consultations: Operations Branch - National Targeting Centre (NTC); Traveller Programs (Policy and Program Management)

CBSA VP/AVP - Programs Branch
RECEIVED/REÇU
23 MARS 2015
ASFC VP/VPD - Direction générale des Programmes

Canada

Canada Border Services Agency | Agence des services frontaliers du Canada

Protected A

For information

UPDATE ON THE GOVERNANCE AND OVERSIGHT FOR SCENARIO BASED TARGETING

For the Vice-President

Richard: good update FYI. PSA 25 3

PURPOSE

This note provides an update on the governance and oversight framework for Scenario Based Targeting (SBT), as per the recommendation made by the Office of the Privacy Commissioner (OPC).

ISSUE

In response to the OPC recommendations, TPU in the Programs Branch has established a framework for more robust and auditable process for monitoring of the SBT program including a process for review of scenarios to ensure they meet legislative, regulatory and privacy requirements.

BACKGROUND

In a response to the OPC in November 14, 2014, the CBSA committed to putting in place program oversight to periodically verify scenarios for proportionality, and potential impacts on privacy, civil liberties and human rights.

STATUS

The "Scenario Based Targeting (SBT) Policy and Governance" document has been finalized in consultation with the NTC and Traveler Air Programs. This document outlines the governance of SBT through two committees that have been established to provide oversight for the SBT scenarios; the Traveler Scenario Management Committee (TSMC) and the Targeting Program Management Committee (TPMC). The TSMC is a working level committee composed of representatives from both the Operations and Programs Branches with responsibility for the scenario development, activation, monitoring, and maintenance and review process. The TSMC reports to the TPMC. The TPMC provides oversight, guidance and horizontal coordination for

Canada

all Targeting related issues and is co-chaired by the Director NTC and the Director Intelligence, Targeting and Criminal Investigations Programs Management. The TPMC reports to the Enforcement and Intelligence Programs Management Committee and, as required, will report issues to the Traveler Program Management Committee. This document also outlines a dispute resolution process to manage risk associated with scenarios that are in potential non-compliance with program requirements. This process has been designed to allow for rapid operational responses to imminent and significant national security or public safety threats by allowing such scenario to go or remain live during an interim period while additional reviews to ensure compliance with program requirements are underway.

NEXT STEPS

The committees, as described in the attached "Scenario Based Targeting (SBT) Policy and Governance" document, will begin formally reporting in Q1 2015/16.

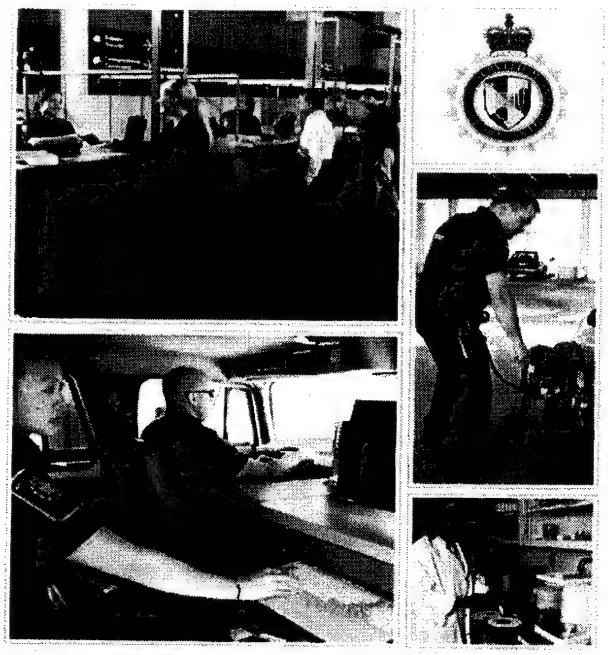
Monik Beauregard, Director General
Enforcement and Intelligence Programs

ATTACHMENT

1. **Scenario Based Targeting Policy and Governance**

CBSA ASFC
PROTECTION • SERVICE • INTEGRITY PROTECTION • SERVICE • INTÉGRITÉ

Scenario Based Targeting (SBT) Policy and Governance



Targeting Program Unit,
Enforcement and Intelligence
Programs Directorate

Programs Branch

Version: 2015-03-19

Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

PREAMBLE

The CBSA Scenario Based Targeting Governance Framework was drafted by the Targeting Program, Intelligence Targeting and Criminal Investigations Division, Programs Branch.

This document has been verified for technical accuracy at the time of publication and requests for additional use must be vetted through the Targeting Program. This document may not be reproduced or distributed without the permission of the Targeting Program. This publication is not intended for external use.

If access is requested under the *Access to Information Act* or *Privacy Act,* no decisions should be taken without prior consultations with the Targeting Program, as the requested information may be subject to exemptions.

Scenario Based Targeting Program Governance Framework

Introduction

Pre-arrival targeting of people travelling to Canada onboard commercial aircraft contributes to the identification and interception of potentially high risk people that may pose a threat to national security, safety and the prosperity of Canada.

Scenario based targeting is the process by which all advance information submitted by commercial airlines or their service providers [Advance Passenger Information (API)/Passenger Name Record (PNR)], is processed through pre-defined scenario based rules in the CBSA Passenger Information System (PAXIS).

Scenarios are generated on the basis of intelligence analysis, anticipated trends or risk patterns that are associated to threats to national security, public safety or other border risks involving contraband or immigration.

Potential high risk passengers are identified for targeting officer review when their personal information matches all the criteria in a scenario. Targeting officers at the National Targeting Centre (NTC) conduct further investigative research to either negate the risk or issue a target which will result in the passenger being referred for secondary examination upon arrival at the port of entry.

The CBSA Scenario Based Targeting Privacy Impact Assessment (PIA) was submitted to the Office of the Privacy Commissioner (OPC) in early 2014. The OPC subsequently recommended that the CBSA establish a governance framework for the review of SBT scenarios for effectiveness and proportionality and to ensure that the scenarios did not unnecessarily impede the civil liberties or human rights of travellers.

Scenario-Based Targeting Governance

The SBT governance framework leverages the existing organizational framework to ensure that leadership, organizational structures, communications and processes are in place to ensure efficiency and effectiveness in the management of the Scenario – Based Targeting (SBT) program and compliance with international agreements and legislative requirements.

Roles and Accountabilities

National Targeting Centre, Operations

The National Targeting Centre, Operations, is accountable for the operational delivery of the SBT program including scenario development and monitoring and performance reporting.

NTC Operations accountabilities include:

- Acting as the Office of Primary Interest for the SBT Program, performing SBT operational procedures maintenance, scenario development and monitoring, performance reporting and the Rules Management Application (RMA) in PAXIS.
- Ensuring all SBT operational procedures, scenarios and other documentation are protected commensurate with CBSA technical, security and organizational procedures.
- Training or communicating to all identified partners in the scenario creation process the standard operating procedures for scenario creation management, monitoring and compliance.
- Maintaining the scenario development tracking log and scenario master list (until the implementation of the electronic scenario library in PAXIS) for inventory, monitoring and control purposes and for program accountability requirements.
- Retaining all targeting scenario proposal templates; tracking and recording all implementation, activation and deactivation of scenarios in the RMA.
- Monitoring and consulting internal partners regarding API/PNR data quality or data provision problems that impact the effectiveness of scenarios or the efficiency of PAXIS.
- Tracking and recording data submission quality and IT related systems issues to inform process improvements and program effectiveness measures.
- Acting as the lead on the development and tracking of collaborative scenarios and shared SBT – related projects with international partners.
- Developing and distributing SBT performance reports to internal stakeholders.
- Ensuring SBT program integrity and all individual SBT scenario legislative and privacy compliance requirements.
- Acting as the OPI for scenario creation and development by NTC Operations and its partners, including Targeting Operations Intelligence, Regional Operations and Regional Enforcement and Intelligence.
- Assuming the responsibility for the scenario lifecycle including: scenario issuance, maintenance, reviewing, reporting and closing, with further responsibilities including:
    - Assessing scenario operational impacts prior to deployment in PAXIS;
    - Reviewing scenario intelligence, the risk environment and new information to judge the relevance of the scenario and to determine if the scenario should remain, be modified or decommissioned from PAXIS;
    - Calibrating the effectiveness of scenarios through research and analysis, consultations with internal / external partners and recording subsequent scenario modifications or deletions;
    - Regularly monitoring individual scenario effectiveness through performance metric analysis
    - Utilizing and maintaining a detailed checklist to maintain an auditable record of scenario compliance review.

Programs Branch, Targeting Programs

The Targeting Program unit, Programs Branch, is the functional authority for the SBT and its accountabilities include:

- Developing and maintaining Scenario Based Targeting Program policies and high level guidelines.
- Coordinating and maintaining records of the SBT Program Management Committee
- Coordinating Targeting and API/PNR Program related systems changes/fixes or projects in conjunction with Business Systems Integration Division.
- Coordinating and providing secretariat support for the scenario review committee. Ensuring reporting and escalation of issues as required on SBT related matters.
- Representing the NTC and Targeting programs' systems, tools, business and process improvements to facilitate operational delivery and ongoing enhancement of SBT and the Targeting Program. (i.e. new systems/applications, analytical tools and processes – e.g. SPSS modeller, data warehouse, etc.).

Programs Branch, Traveller Programs, Air Programs Unit

The Air Programs Unit accountabilities include:

- Provision of program strategy and policy direction related to the collection and use of Advance Passenger Information / Passenger Name Record (API/PNR)
- Development and maintenance of related policies, regulations, and legislation;
- Control and approval of requests for access to the PAXIS system

Governance Committees

Traveler Scenario Management Committee

Monthly meetings focused on the operational coordination of scenario development, activation, monitoring, and maintenance and review process. Manager and officer level representative from the NTC units, IOAD, and both the Targeting and Intelligence Programs units. Other areas may participate on an ad hoc basis as required. These members will have the following responsibilities:

- Review scenarios for effectiveness and make recommendations for deactivation or modification, as appropriate
- Review and finalize scenario project proposals/plans
- Review and recommend amendments to scenario development and management processes and procedures as required
- Disseminate information/recommendations to their respective areas, as required
- Share scenario development best practices and lessons learned

- Identify and recommend solutions to issues that impact the SBT process (ex: data quality, provision, review rates, 600 scenario limit, elements for coding)
- NTC TTSIR will act as secretariat including agenda development and maintaining records of discussion
- Refer issues, as required, to the Targeting Program Management Committee

Targeting Program Management Committee

Monthly meetings co-chaired between senior officer and manager level representatives from the NTC, E&I Programs Management, Traveler Policy and Program Management, Commercial Policy and Program Management and Business Systems Integration with accountability for ensuring horizontal program coordination for all aspects of the targeting program. With regards to the SBT, the committee will have the following accountabilities:

- Monitoring and periodically reviewing SBT scenarios, SBT performance measurement and accountability requirements, PAXIS and API/PNR data quality issues and airline data submission compliance rates
- Developing, reviewing or recommending SBT policy, procedures, guidelines, processes and system requirements
- Identifying, analyzing and proposing solutions for any SBT program or SBT scenario issues.
- Providing reporting and recommendations to the Directors of the NTC, E&I Programs Management and Traveler Programs Divisions on issues concerning SBT

Directors NTC, E&I Programs Management and Traveler Policy and Program Management Divisions

The Directors will meet as required and are accountable to:

- Provide leadership, oversight and guidance to the SBT and the program management committee
- Engage additional program areas as required (i.e. Business Systems Integration)
- Provide ongoing reporting to the PMTs on SBT program performance
- Refer recommendations as required to the relevant DGs/VPs for decision
- Ensure disputes follow the established resolution process

Enforcement and Intelligence PMT and Traveler PMT

Issues will be referred to the E&I PMT, the Traveler PMT or both as required.

The Chair and Co-Chair of the PMT are accountable for providing guidance and direction to the responsible Directors as follows:

- Ensuring strategic planning and horizontal communications with regards to the SBT
- Providing guidance on Implementing and monitoring performance measures

- Identifying and leveraging best practices for the SBT
- Reviewing program costs and identifying opportunities for savings within the SBT
- Ensuring overall alignment with agency priorities or long-term planning

SBT Scenario Dispute Resolution

Where there is a dispute regarding the policy compliance or legislative authority to initiate a specific scenario, the Travel Scenario Management Committee or its members will notify the co-chairs of the Targeting Program Management Committee as soon as practical.

The Directors will seek to develop consensus on the dispute and provide direction to the Program Management Committee accordingly.

Should the Directors fail to reach consensus, a joint briefing to the relevant DGs and VPs (as required) will be prepared by the Director, E&I Programs Management.

For all disputes regarding an SBT scenario with imminent and significant national security or public safety implications, the scenario will either be activated or remain in the PAXIS system until such time as the dispute is resolved.

In all other cases the Program Management Committee will inform the Directors of the scenario proposal and delay the implementation of the scenario until it is has received Director level approval.

Appendix A

Committee Structures

Traveler Scenario Management Committee

- National Targeting Centre
- Intelligence Operations and Analysis Division
- Intelligence, Targeting and Criminal Investigations Programs Management Division
- NTC TTSIR - Secretariat

Targeting Program Management Committee

- Intelligence, Targeting and Criminal Investigations Programs Management Division
- National Targeting Centre
- Traveler Programs, Air Programs
- Commercial Programs
- Business Systems Integration
- Targeting Policy Unit – Secretariat

Enforcement and Intelligence PMT

- Enforcement and Intelligence Programs
- Enforcement and Intelligence Operations
- National Targeting Centre
- International Operations
- Traveller Programs
- National Targeting Centre
- Program Policy and Coordination
- Pacific Region
- Training & Learning, Human Resources Branch
- Corporate Governance & Accountability, Corporate Affairs Branch
- Enterprise Architecture and Information Management, IST Branch
- Resource Management Directorate, Comptrollership Branch
- Transformation and Oversight, Comptrollership Branch

Traveler PMT

- Traveler Programs
- Traveler Operations
- NTC
- IST Branch
- Recourse
- Resource Management Directorate, Comptrollership Branch
- Pacific Region
- GTA Region

  Atlantic Region

Traveller Scenario Management Committee
Terms of Reference

Context/Background:

Scenario Based targeting (SBT) is a key part of the Canada Border Service Agency's (CBSA's) pre-arrival traveller targeting program and supports the Agency's Risk Assessment Program by contributing to the identification and interception of suspected potential high and unknown risk people that may pose a threat to the national security, safety and prosperity of Canada. It also fulfils a commitment made by the CBSA under the Beyond the Border Action Plan to implement an enhanced SBT targeting methodology similar to that of the US Customs and Border Protection.

Increasing targeting work volumes, finite resources, ongoing scrutiny of standardized/automated risk assessment and border security approaches and ever-changing risks/threats necessitate ongoing robust rigour and scrutiny of the CBSA's risk management and assessment tools such as pre-arrival targeting's SBT process.

- At the heart of SBT are the scenarios. In order to ensure the integrity and effectiveness of SBT and the overall success of the CBSA's traveller targeting program, the effectiveness of scenarios and the efficiency and integrity of their development and management processes/procedures needs to be regularly reviewed and adjustments made as required.

Prior to the Programs Branch realignment in June 2014, Targeting Programs was responsible for SBT scenario development/implementation, management/maintenance, monitoring. Responsibility for all these activities was transferred to the National Targeting Centre (NTC) - Operations Branch as part of the realignment. Targeting Programs provides oversight for the CBSA's Targeting Program.

Mandate/Expected Outcome

Conduct ongoing review of scenarios and scenario development and management processes/procedures to ensure scenario effectiveness, development and management process/procedural efficiency, consistency and integrity. Scenarios deemed ineffective may be deactivated or modified, and processes/procedures will be updated as required. The committee will also review and finalize potential scenario effectiveness assessment proposals/plans.

Membership*

Initially will include applicable NTC team representatives, but will be expanded to include Targeting/Intelligence Programs and Intelligence Operations and Analysis Directorate (IOAD), and other areas as required. Guests (e.g. IT) will be invited to speak to specific topics as required.

Chair – NTC	Paul Porrior, Director
Co-Chair: NTC	Curtis Young, TRIS Manager
Secretariat:	Targeting Rules Indicators and Scenarios (TRIS)

Representatives

NTC:	
NTC – Targeting Intelligence (TI)	Tom Toulouse, Francesca Macchione, David Whetstone
NTC – Traveller Targeting (TT)	Marc Beauvais, Philip Crabbe, Natalie Rocque
NTC – TRIS	Kelly Cummings, Lauren Berrigan
NTC- Data Analytics Unit (DAU)	Mohamed Migahed
Targeting Programs	Melissa Wigham; Jo-Ellen Langevin

*Members require Secret clearance and a working knowledge of SBT.

Meeting Frequency

Monthly

Members Roles and Responsibilities

- Review scenarios for effectiveness and make recommendations for deactivation or modification as appropriate.
- Review and finalize scenario effectiveness assessment proposals/plans.
- Review and make amendments to scenario development and management processes and procedures as required.
- Disseminate information/recommendations to their respective areas, as required.
- Share scenario development best practices and lessons learned.
- Discuss issues that impact the SBT process (ex: data quality, provision, review rates, scenario capacity limit, elements for coding).

TRIS

- Draft proposals for scenario effectiveness assessments
- Present findings on scenario effectiveness.

- Lead scenario review, effectiveness assessment proposal and process improvement discussions.
- Present items for discussion.

Meeting Organization

- A program officer from TRIS, NTC will act as meeting Coordinator.
- Working group meetings will be held once a month for approximately 2 hours. May be held more often as required.
- Selection of scenarios for review and associated performance analysis reports will be prepared by TRIS for discussion at the meeting.
- Records of discussion will be drafted and shared by the Coordinator.

CBSA ASFC

PROTECTION · SERVICE · INTEGRITY

CBSA's Contribution to Aviation Security – A Targeting Point of View

Risk Assessment Programs
HINT Conference
May 20, 2010

Canada Border Services Agency / Agence des services frontaliers du Canada

Canada

CBSA's Contribution to Air Security – A Targeting Point of View

- Current targeting initiatives
  - API/PNR Program
  - National Security Targeting
- Work underway
  - National Risk Assessment Centre focus
  - System changes and enhancements
  - Risk Analysis
  - Targeting Program
  - Targeting Service Delivery
- Future initiatives
  - Pushing the Border Out

API/PNR Program

- The Advance Passenger Information/Passenger Name Record (API/PNR) program is designed to protect Canadians by enabling the Canada Border Services Agency (CBSA) to perform a risk assessment of travellers prior to their arrival in Canada to identify those who require further examination upon arrival
- API/PNR may be used for the purpose of identifying persons who are or may be involved with or connected to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature
- The API/PNR program is the cornerstone to Canada's and the CBSA's air security program

CBSA ASFC

Program Implementation

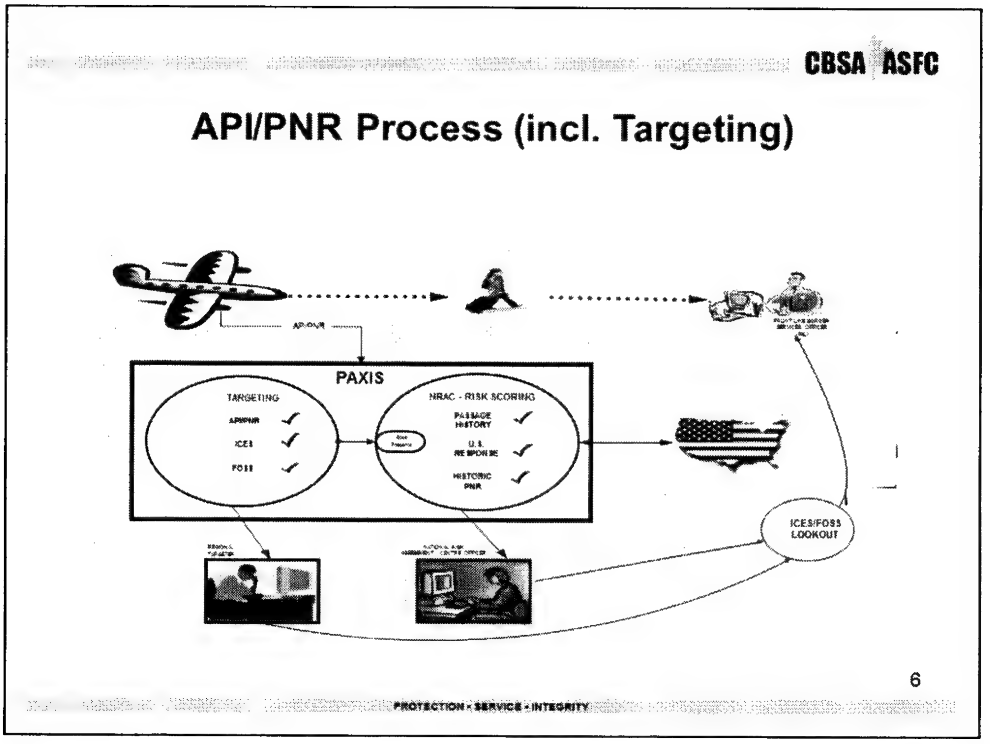
- The CBSA took a phased-in implementation approach to the API/PNR program:
  - Implementation of the API component of the program commenced on October 7, 2002 (6 months to develop and implement)
  - Implementation of the PNR component of the program commenced on July 8, 2003
  - Other system components have been delivered through the years
-
-
- The National Risk Assessment Centre (NRAC) opened its doors in 2005

4

PROTECTION • SERVICE • INTEGRITY

Passenger Information System (PAXIS)

- PAXIS receives, stores and risk assesses all people for whom API/PNR is collected by the CBSA
  - PAXIS has a robust technical infrastructure that provides an opportunity for functionality expansion
- As per the Agreement with the European Union and Canada's legislation and regulations, all data defined as API or PNR must be stored only in the PAXIS system
- API and PNR data can be stored for a maximum of 3.5 years.
- As part of the PNR Push project, PAXIS and the data acquisition components are being extensively re-engineered
  -
  -



Information arriving in PAXIS is risk assessed in two stages:

API received by CBSA is automatically queried against the CBSA's Integrated Customs Enforcement System (ICES) and Field Operation Support System (FOSS).

Results are available to the National Risk Assessment Centre (NRAC) users and targeters in the local airport targeting units.

Automated risk scoring process via algorithms, is done,

Risk-scoring results are only available to NRAC users.

Includes a component where a limited data set of information (for high risk travellers) is automatically shared with the US CBP. (Request for Information – RFI)

An automated process is available to share lookouts between Canada and the US.

Scenario Based Targeting

- Moving to a fully automated scenario based targeting process continues
- Improvements and enhancements to all parts of the process including:
  - Enhancing the CBSA capability to develop scenarios based upon trends analysis
  - Providing direction to front line employees on the new approach for national security including providing information and support for the examination and interview process (rule focus)
- Expanding scenarios and enhancing technology
  - Short Term
    - Expanding targets
  - Medium Term
    - Improved technology
  - Long Term
    - Full technological solution with rule test environment

CBSA's Targeting Program

- CBSA's full commitment to improve and enhance targeting by establishing a functional authority focused on targeting
- A working group identified recommendations to improve targeting program including the possibility of a new targeting service delivery model
- Increased focus will provide a more coherent approach to identifying high risk travellers and goods
- Plans for future investments in the program including technology changes and expansion to other modes
- Development of performance measurements to ensure the program is working

Where does CBSA go next?

- The Border Management Action Plan under development (part of the CBSA Change Initiative) identifies pushing the borders out as a key element in the CBSA multi-layered approach strategy
- CBSA fully supports a "board-no board" process for air travellers
- Continuing to move ahead in an environment of fiscal restraint presents its challenges
- The CBSA continues to push the concept as a better way to identify high-risk travellers and increase efficiencies

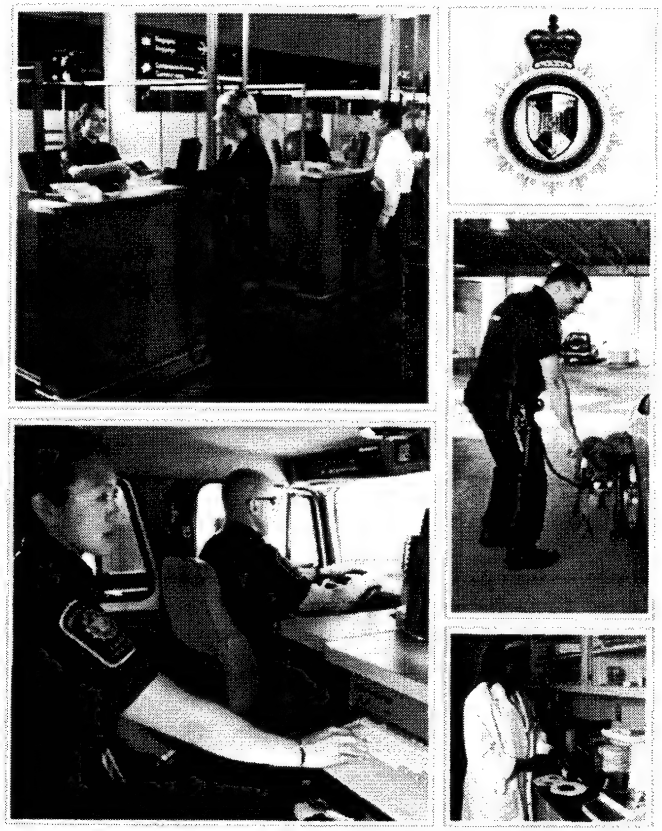
CBSA ASFC

PROTECTION • SERVICE • INTEGRITY

PROTECTION • SERVICE • INTÉGRITÉ

Enforcement Activities:

Canada's API/PNR Program



October 2014

Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

Canada's API/PNR Program – Overview

- Canada began requiring Advance Passenger Information (API) in 2002 and Passenger Name Record (PNR) data in 2003 from commercial air carriers.

- This data is collected by the Canada Border Services Agency (CBSA) whose mandate is to provide integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods.

- The CBSA uses this data to identify persons with a potential relationship to terrorism or serious transnational crime.

Targeting – Overview

- Basic identifying information collected as API is used to identify all travellers who present a 'known' risk.
  - Provided by commercial airline carriers
  - Run against CBSA's enforcement systems to match any previous enforcement history.

- Reservation information, or PNR, is used to evaluate 'unknown risk'.
  - Provided by commercial airline carriers
  - Run against algorithms to match inbound travellers against pre-determined scenarios.

- The targeting officer then reviews scenario matches and analyses the available passenger information of each suspected high-risk traveller to determine whether or not a target should be issued.

- The CBSA uses a Scenario-Based Targeting methodology,

Targeting Scenarios

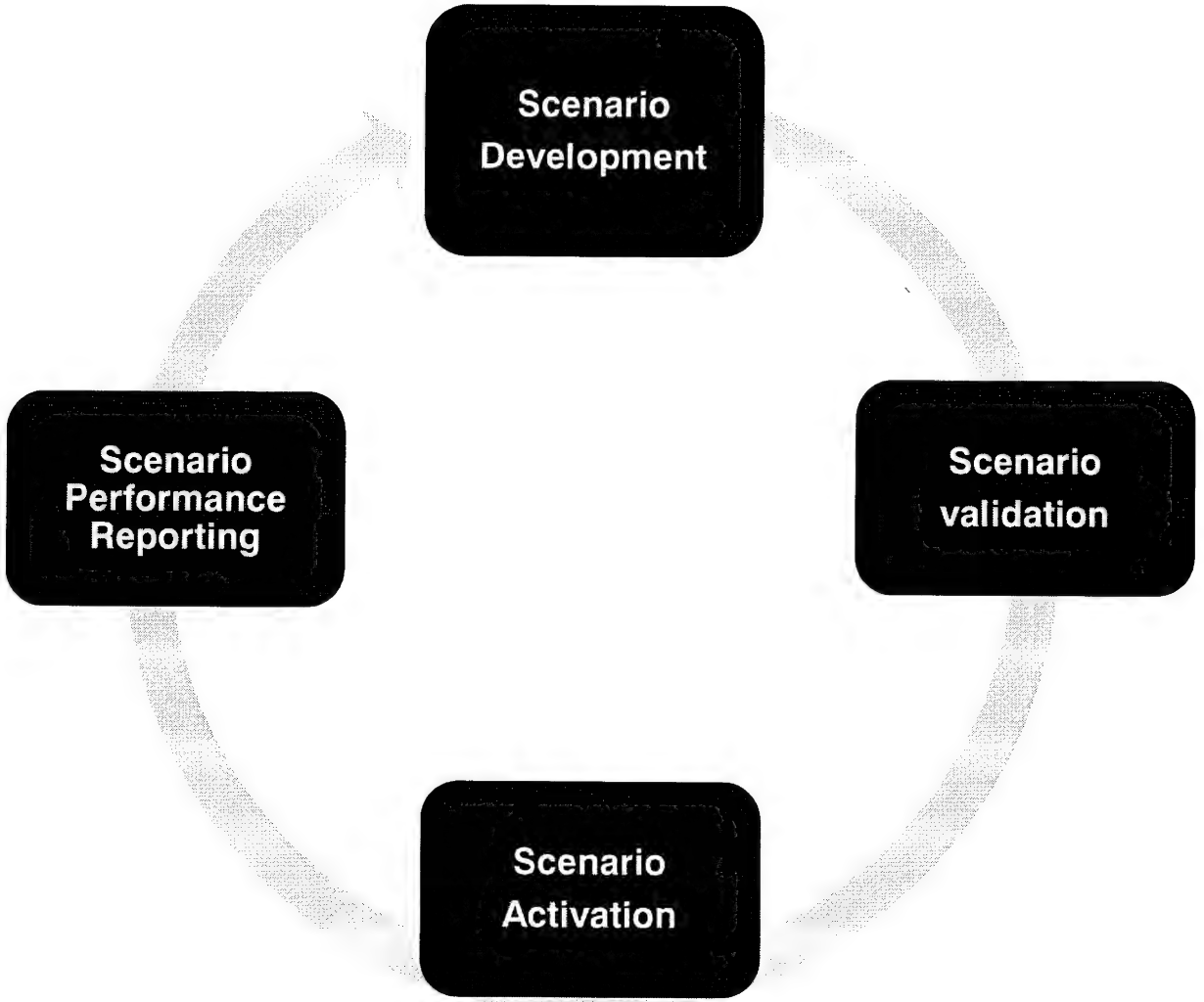
What is a Scenario?

- A set of characteristics identified using PNR data that indicate that a traveller may pose a threat.

How a Scenario is created?

- Intelligence reveals a risk through trend analysis an investigation.
- The parameters of a traveller likely to be linked to the threat are identified.
- The scenario is created in the CBSA system and analysed to determine potential hit rate and effectiveness
- If this analysis is successful, the new scenario is activated.

SBT Scenario Development - Process Flow



The Targeting Officer

What is the role of the targeting officer?

- They review each traveller on the scenario match worklist and either confirm or negate the risk.
- Targeting officers have access to a variety of additional data sources for further investigation
- If the officer believes that the traveller poses a likely threat, a target is issued for further examination upon arrival in Canada
- The target issued will contain details and the rationale for issuing the target to assist the examining officer in their questioning.
-

Enforcement and Intelligence

- The CBSA uses API/PNR information after the arrival / examination of passengers for intelligence purposes.
- Historical PNR information and targeting results are analysed to identify trends and build future targeting scenarios in response.
- The information is also used for specific investigations.

Contact Information

General enquiries regarding Canada's API/PNR program:

api-pnr@cbsa-asfc.gc.ca

API/PNR policy and program related enquiries:

kathy.therien@cbsa-asfc.gc.ca

+1 613 954 1155

Thank you

Questions?

Scenario Based Targeting Overview

July 23, 2014

Overview

- Targeting Program Overview
- Targeting Process Overview
- What is Scenario Based Targeting (SBT)?
  - Process and data elements
- How are scenarios developed?
  - Sources
  - Categories
  - Scenario Development- Steps
  - Closing the Loop
- SBT Benefits
- Future Vision and Initiatives

Targeting Program Overview

- Objective - to identify high-risk travellers prior to their arrival in Canada by :
  - Intercepting those who may pose a threat to Canada's safety and security;
  - Enacting more successful examinations; and,
  - Facilitating entry of lower risk travellers and goods.

- Support for CBSA's Strategic Priorities:
  - Targeting higher risks as early as possible in the travel, immigration and supply chain continuums;
  - Ensuring Canada's population is safe and secure from border-related risks.

- Supporting sound border management through the use of risk assessment and targeting processes;

- The CBSA's Targeting Operations are delivered centrally at the National Targeting Centre (NTC) in Ottawa, on a 24/7 basis.

Targeting Defined

The Canada Border Services Agency defines:

Targeting - The process of identifying suspect high-risk people, goods and conveyances through a deductive reasoning process utilizing advance information, technology and intelligence products.

Target – A target is a type of referral using advance information that identifies suspect high-risk people, goods and conveyances that may pose a risk to national security and/or public safety priorities

Targeting

Targeting:

- Considers unknown risk, rather than the known;
- Identifies suspect high-risk people;
- Leverages indicators, intelligence products, deductive reasoning;
- Alerts appropriate CBSA personnel of an impending suspected risk to ensure interception.

Targeting Process Overview

- Airlines and service providers electronically transmit the mandatory API/PNR data to the CBSA;
- The API/PNR undergoes an automated risk assessment that uses enforcement databases and scenarios to identify known and potential risk;
- Targeting Officers review those travellers identified as high-risk to either confirm or negate the risk;
- If risk cannot be negated, the targeting officer will issue a target to the appropriate port of entry for interception upon their arrival;
- All interception results are subsequently reviewed to monitor or update the existing risk assessment criteria.

What is Scenario Based Targeting?

What is Scenario Based Targeting?

- Scenario Based Targeting (SBT) is an automated process. The API/PNR of all travellers is compared with pre-determined sets of data elements in order to identify potential high risk travellers prior to their arrival in Canada.

- A "**Scenario**" is a grouping of specific data elements, or indicators, derived from various sources and can reflect an identified trend or pattern.

- Scenarios can be developed for any risk type

- If elements of a traveller's information match the same elements in a scenario, the traveller is selected for review

- The use of scenarios allows the CBSA to better focus on potentially high risk travellers.

What is Scenario Based Targeting?

- SBT helps the focus targeting efforts on potentially high risk travellers
- SBT helps targeting officers by automatically filtering all travellers (all flights) and shortlisting only the high risk travellers for comprehensive review.
- Every traveller's API/PNR, when received by the CBSA, will be processed through scenarios; if a traveller meets a pre-determined scenario, they will be placed on a work list for review
- After reviewing the traveller using internal and external sources, the Targeting Officer will decide whether or not to issue a target on the traveller for further examination once they arrive in Canada.

Advance Passenger Information (API) Data Elements

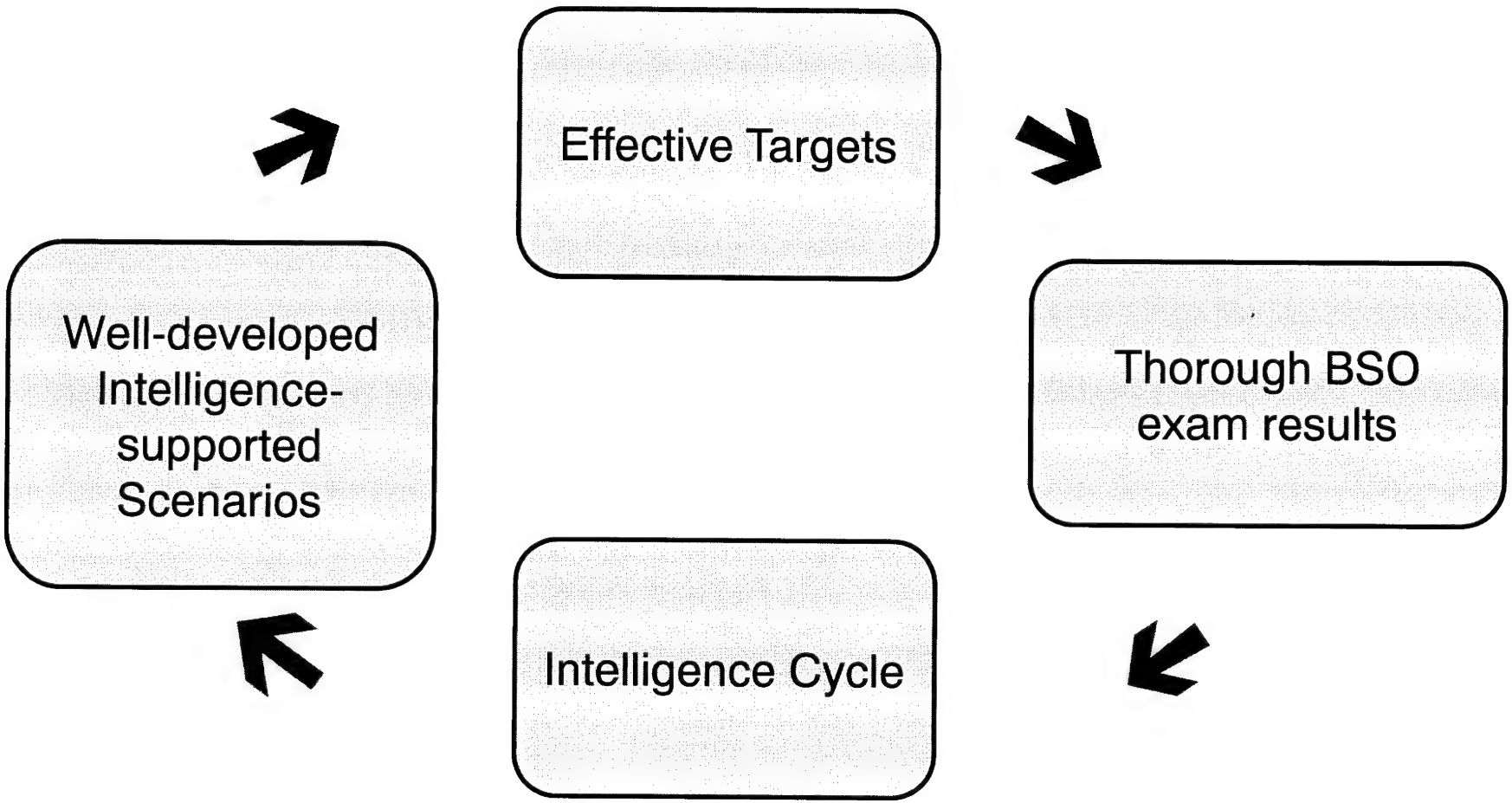
- API is data identifying the person, including full name, date of birth, gender, citizenship, travel document type and number and country of issue.
- The CBSA requires air carriers to provide the following information about each person on board :
  - surname, first name and initial or initials of any middle names;
  - date of birth;
  - the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;
  - gender;
  - passport or travel document number;
  - reservation record locator or file number.

Passenger Name Record (PNR) Data Elements

PNR is data with respect to a person's travel itinerary, contained within a commercial carrier's reservation system, created once a person makes a reservation.

a) PNR Locator Number (e.g. Booking Reference and/or Tracking Number(s);
b) Dates of Reservation and Intended Travel;
c) Passenger Name;
d) Other Names on PNR;
e) All Forms of Payment Information (e.g. Cash, Cheque, Frequent Flyer Point Rewards);
f) Billing Address;
g) Contact Telephone Numbers;
h) All Travel Itinerary for Specific PNR (e.g. All Itinerary Cities, Non-air Segments and Connection Details);
i) Frequent Flyer Information (e.g. Frequent Flyer Number);
j) Travel Agency and Travel Agent Information (e.g. Agency IATA Number and Agent Contact Information);
k) Split/Divided PNR Information;
l) Ticketing Information (e.g. One-Way Tickets, Exchange Ticket, Ticket Number(s) and Date of Issuance);
m) Seating Information, (e.g. Class of Service, Seat Number, Seating Preference)
n) Go Show & No Show Information (i.e. No reservation, or did not Check-in);
o) Baggage Information (e.g. Number of Bags and Bag Weight);
p) Any Collected API Information;
q) Standby Information (e.g. Waiting for Seat Availability Indicator); and
r) Check-In Information (eg. Boarding Indicator and Check-in Order).

How are scenarios developed?



Scenario Sources

Information from the following sources can be considered in the development of a scenario:

Sample Scenario Categories

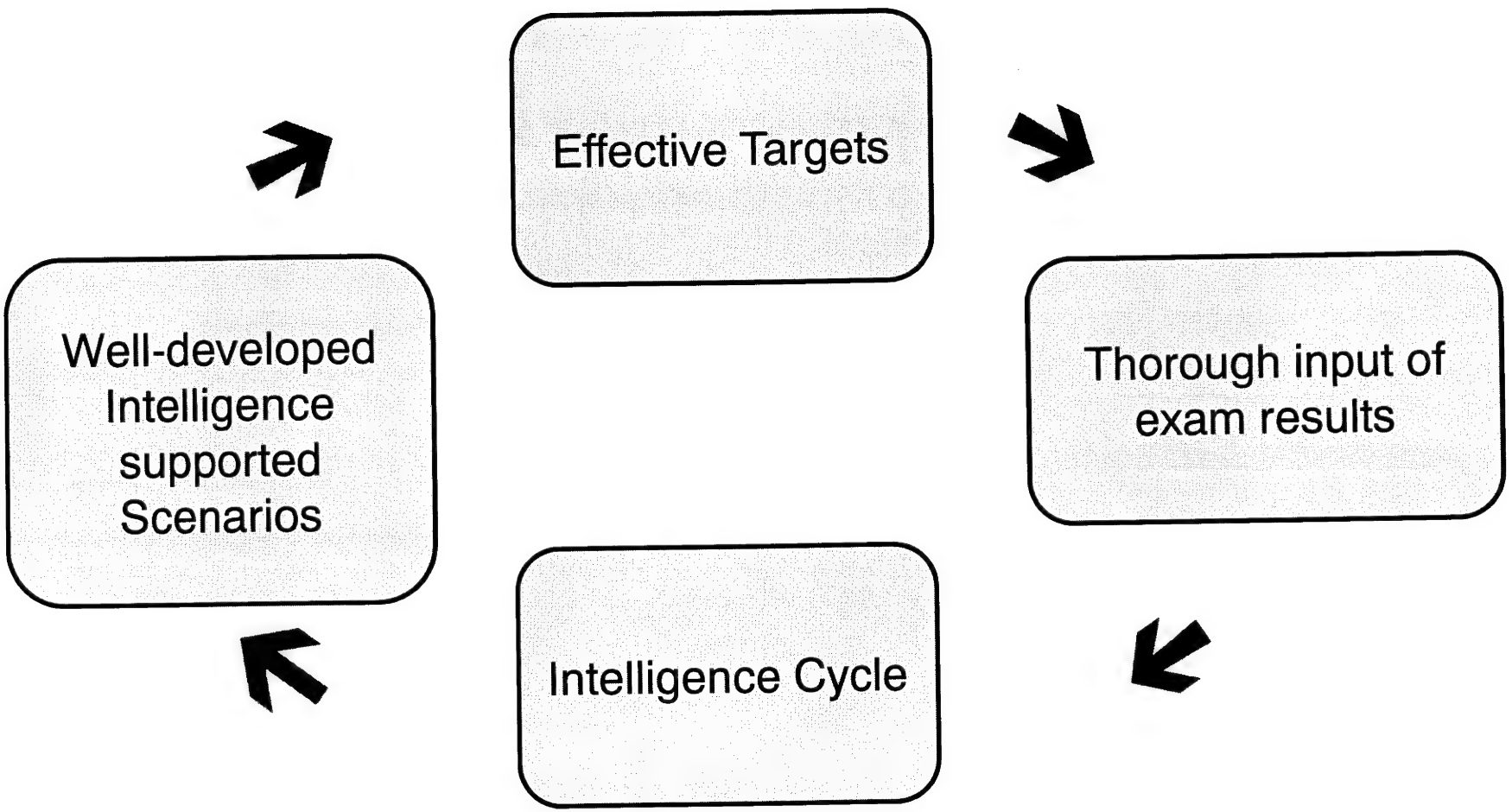
Scenario Development- Steps

- Intelligence received from various sources
- Information is analyzed to determine if intelligence is relevant, timely, and actionable
- New scenario is proposed and verified for alignment with legislation, regulations, policy, priorities
- Input/activate scenarios
- Effectiveness of scenarios is monitored regularly and amended or revised as necessary

Closing The Loop

- Detailed statistics maintained on target issuance, PNR and examination results
- Examination results are tracked
- Communication protocol established to obtain missing or incomplete examinations reports
- All missed targets are reviewed to determine rationale for missed intercept
- Significant results from targets are communicated within the NTC for information sharing, intelligence analysis and reporting purposes
- Monthly National/ Regional targeting performance reports

Protected B



Scenario Based Targeting Benefits

- SBT screens all inbound air travellers on all flights, and identifies those travellers who warrant further risk assessment. The automated SBT process produces a list of potentially high-risk travellers.
- The work list of higher risk travellers allows Targeting and Field Operations resources to focus on individuals of highest risk.
- New scenarios can be developed in a timely manner to address new and evolving security and enforcement threats.
- These activities expedite the movement of low-risk travellers, and provide a relevant level of certainty that the travellers are actually of low-risk.

Scenario Based Targeting Benefits

- SBT furthers CBSA's international partnerships through sharing and collaboration

- Furthers CBSA's domestic partnerships through consultation and collaboration with key federal and domestic law enforcement partners

Protected B

Scenario Based Targeting Future Vision

Future Initiatives

- Three new CBSA initiatives will make use of API/PNR data:
  - **Interactive Advance Passenger Information (IAPI)** will use API data sent by commercial air carriers in advance of departure to stop inadmissible passengers from travelling to Canada.
  - **Entry/Exit** will use API data from commercial air carriers departing Canada to reconcile entry records. This will enable the CBSA to identify individuals who have overstayed visas or failed to meet residency requirements.
  - **eManifest** will use API data on the crew of commercial cargo conveyances to support the risk assessment of commercial cargo.

Questions

Contact:

Melissa Wigham
Manager
Targeting Unit
Enforcement and Intelligence Programs Directorate
Melissa.Wigham@cbsa-asfc.gc.ca

or

Scenario Based Targeting Overview

September 18, 2014

Overview

- Targeting Program Overview
- Targeting Process Overview
- What is Scenario Based Targeting (SBT)?
  - Process and data elements
- How are scenarios developed?
  - Sources
  - Categories
  - Scenario Development- Steps
  - Closing the Loop
- SBT Benefits
- Future Vision and Initiatives

Targeting Program Overview

- Objective - to identify high-risk travellers prior to their arrival in Canada by :
  - Intercepting those who may pose a threat to Canada's safety and security;
  - Enacting more successful examinations; and,
  - Facilitating entry of lower risk travellers and goods.

- Support for CBSA's Strategic Priorities:
  - Targeting higher risks as early as possible in the travel, immigration and supply chain continuums;
  - Ensuring Canada's population is safe and secure from border-related risks.

- Supporting sound border management through the use of risk assessment and targeting processes;

- The CBSA's Targeting Operations are delivered centrally at the National Targeting Centre (NTC) in Ottawa, on a 24/7 basis.

Targeting Defined

The Canada Border Services Agency defines:

Targeting - The process of identifying suspect high-risk people, goods and conveyances through a deductive reasoning process utilizing advance information, technology and intelligence products.

Target – A target is a type of referral using advance information that identifies suspect high-risk people, goods and conveyances that may pose a risk to national security and/or public safety priorities

Targeting

Targeting:

- Considers unknown risk, rather than the known;
- Identifies suspect high-risk people;
- Leverages indicators, intelligence products, deductive reasoning;
- Alerts appropriate CBSA personnel of an impending suspected risk to ensure interception.

Targeting Process Overview

- Airlines and service providers electronically transmit the mandatory API/PNR data to the CBSA;
- The API/PNR undergoes an automated risk assessment that uses enforcement databases and scenarios to identify known and potential risk;
- Targeting Officers review those travellers identified as high-risk to either confirm or negate the risk;
- If risk cannot be negated, the targeting officer will issue a target to the appropriate port of entry for interception upon their arrival;
- All interception results are subsequently reviewed to monitor or update the existing risk assessment criteria.

CBSA - Released under the Access to Information Act.
ASFC - Divulgation en vertu de la loi sur l'Accès à l'information.

Protected A

What is Scenario Based Targeting?

What is Scenario Based Targeting?

- Scenario Based Targeting (SBT) is an automated process. The API/PNR of all travellers is compared with pre-determined sets of data elements in order to identify potential high risk travellers prior to their arrival in Canada.
- A "**Scenario**" is a grouping of specific data elements, or indicators, derived from various sources and can reflect an identified trend or pattern.
- Scenarios can be developed for any risk type
- If elements of a traveller's information match the same elements in a scenario, the traveller is selected for review
- The use of scenarios allows the CBSA to better focus on potentially high risk travellers.

What is Scenario Based Targeting?

- SBT helps the focus targeting efforts on potentially high risk travellers
- SBT helps targeting officers by automatically filtering all travellers (all flights) and shortlisting only the high risk travellers for comprehensive review.
- Every traveller's API/PNR, when received by the CBSA, will be processed through scenarios; if a traveller meets a pre-determined scenario, they will be placed on a work list for review
- After reviewing the traveller using internal and external sources, the Targeting Officer will decide whether or not to issue a target on the traveller for further examination once they arrive in Canada.

Advance Passenger Information (API) Data Elements

- API is data identifying the person, including full name, date of birth, gender, citizenship, travel document type and number and country of issue.
- The CBSA requires air carriers to provide the following information about each person on board :
  - surname, first name and initial or initials of any middle names;
  - date of birth;
  - the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;
  - gender;
  - passport or travel document number;
  - reservation record locator or file number.

Passenger Name Record (PNR) Data Elements

PNR is data with respect to a person's travel itinerary, contained within a commercial carrier's reservation system, created once a person makes a reservation.

a) PNR Locator Number (e.g. Booking Reference and/or Tracking Number(s);
b) Dates of Reservation and Intended Travel;
c) Passenger Name;
d) Other Names on PNR;
e) All Forms of Payment Information (e.g. Cash, Cheque, Frequent Flyer Point Rewards);
f) Billing Address;
g) Contact Telephone Numbers;
h) All Travel Itinerary for Specific PNR (e.g. All Itinerary Cities, Non-air Segments and Connection Details);
i) Frequent Flyer Information (e.g. Frequent Flyer Number);
j) Travel Agency and Travel Agent Information (e.g. Agency IATA Number and Agent Contact Information);
k) Split/Divided PNR Information;
l) Ticketing Information (e.g. One-Way Tickets, Exchange Ticket, Ticket Number(s) and Date of Issuance);
m) Seating Information, (e.g. Class of Service, Seat Number, Seating Preference)
n) Go Show & No Show Information (i.e. No reservation, or did not Check-in);
o) Baggage Information (e.g. Number of Bags and Bag Weight);
p) Any Collected API Information;
q) Standby Information (e.g. Waiting for Seat Availability Indicator); and
r) Check-In Information (eg. Boarding Indicator and Check-in Order).

How are scenarios developed?

Scenario Sources

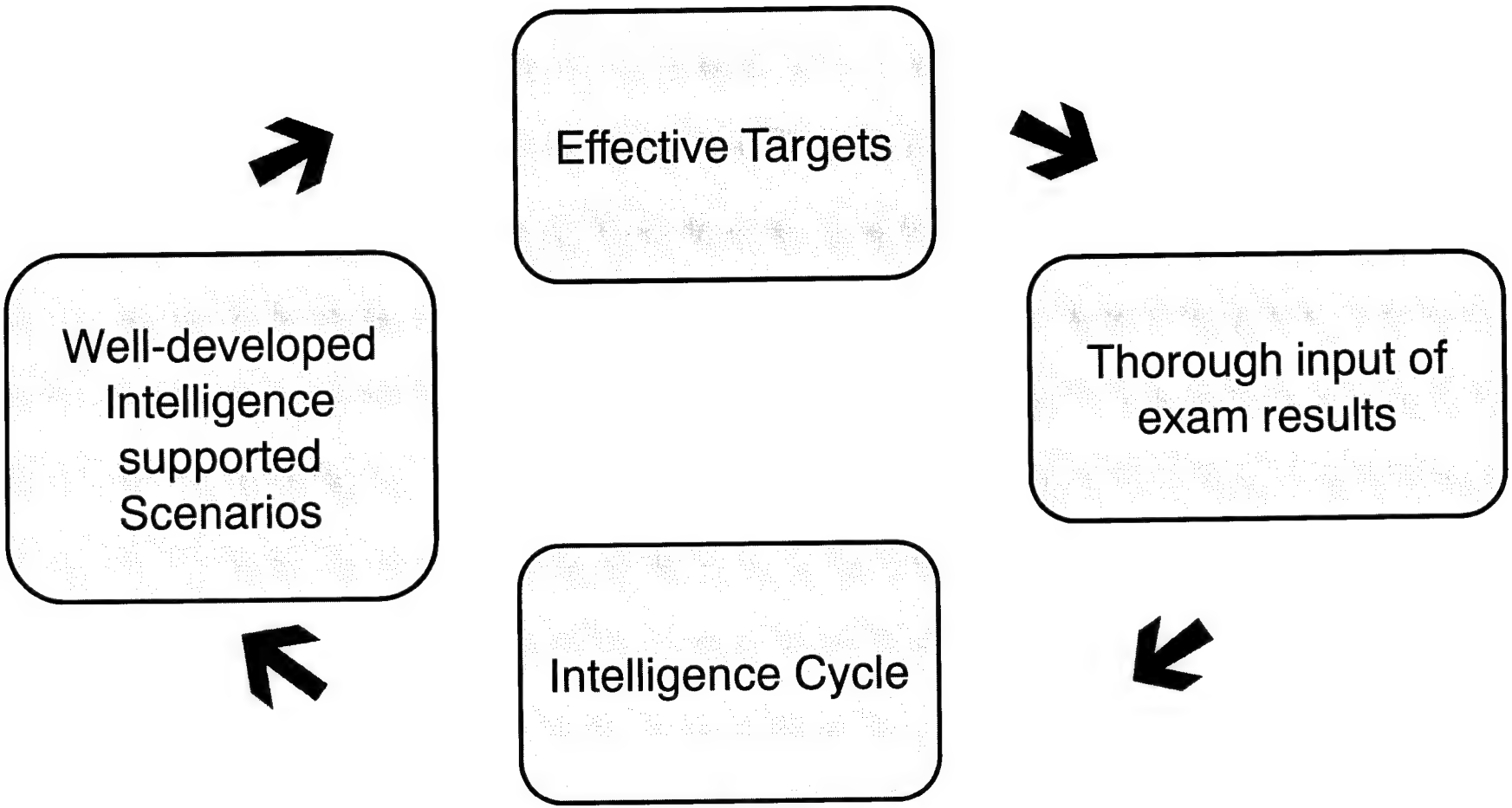
Information from the following sources can be considered in the development of a scenario:

Sample Scenario Categories

Scenario Development- Steps

Closing The Loop

Protected B



Scenario Based Targeting Benefits

- SBT screens all inbound air travellers on all flights, and identifies those travellers who warrant further risk assessment. The automated SBT process produces a list of potentially high-risk travellers.
- The work list of higher risk travellers allows Targeting and Field Operations resources to focus on individuals of highest risk.
- New scenarios can be developed in a timely manner to address new and evolving security and enforcement threats.
- These activities expedite the movement of low-risk travellers, and provide a relevant level of certainty that the travellers are actually of low-risk.

Scenario Based Targeting Benefits

- SBT furthers CBSA's international partnerships through sharing and collaboration

- Furthers CBSA's domestic partnerships through consultation and collaboration with key federal and domestic law enforcement partners

Protected B

Scenario Based Targeting Future Vision

Future Initiatives

- Three new CBSA initiatives will make use of API/PNR data:
  - **Interactive Advance Passenger Information (IAPI)** will use API data sent by commercial air carriers in advance of departure to stop inadmissible passengers from travelling to Canada.
  - **Entry/Exit** will use API data from commercial air carriers departing Canada to reconcile entry records. This will enable the CBSA to identify individuals who have overstayed visas or failed to meet residency requirements.
  - **eManifest** will use API data on the crew of commercial cargo conveyances to support the risk assessment of commercial cargo.

Questions

Contact:

Melissa Wigham
Manager
Targeting Unit
Enforcement and Intelligence Programs Directorate
Melissa.Wigham@cbsa-asfc.gc.ca

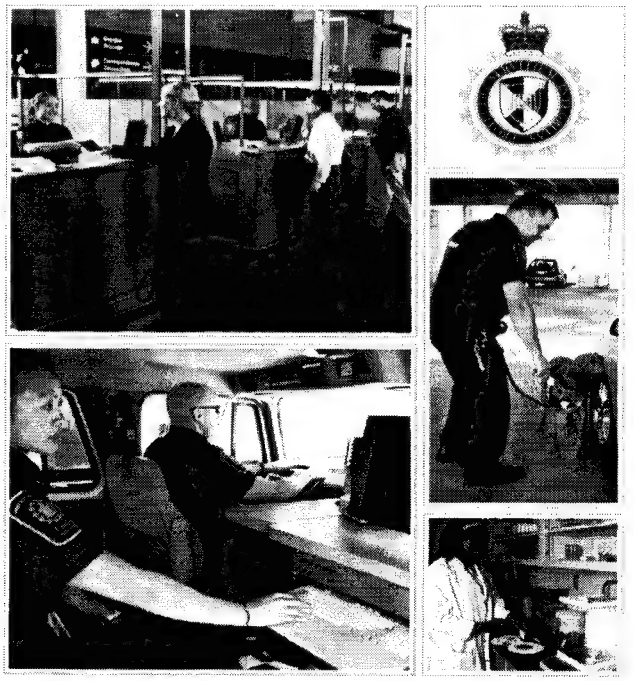
or

CBSA ASFC

PROTECTION • SERVICE • INTEGRITY

PROTECTION • SERVICE • INTÉGRITÉ

Scenario-Based Targeting Governance Framework



Targeting Program,
Enforcement and Intelligence
Programs Directorate

Programs Branch

Version: 2016-11-14

Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

PREAMBLE

The CBSA Scenario Based Targeting Governance Framework was drafted by the Targeting Program, Intelligence, Targeting and Criminal Investigations Division, Programs Branch.

This document has been verified for technical accuracy at the time of publication and requests for additional use must be vetted through the Targeting Program. This document may not be reproduced or distributed without the permission of the Targeting Program. This publication is not intended for external use.

If access is requested under the *Access to Information Act* or *Privacy Act,* no decisions should be taken without prior consultations with the Targeting Program, as the requested information may be subject to exemptions.

Table of Contents

Scenario-Based Targeting Governance Framework

Introduction

The Targeting Program identifies people and goods bound for Canada that may pose a threat to the security and safety of the country. The CBSA uses automated advance information from commercial air carriers to identify people that may pose a threat to Canada. Air carriers are required under the Customs Act and the Immigration and Refugee Protection Act to provide Advance Passenger Information (API) and all available Passenger Named Record (PNR) data about all passengers to the CBSA before a flight's arrival in Canada. International agreements and regulations restrict Canada's use of PNR data to preventing and detecting terrorist offences or serious transnational crime while ensuring scenarios do not contain sensitive data, intrude on privacy or violate civil liberties and human rights.

All air travellers are screened automatically through Scenario-Based Targeting (SBT) whereby the API and PNR data is processed through pre-defined scenario based rules in the CBSA Passenger Information System (PAXIS).

Potentially high-risk travellers are identified for targeting officer review when their API/PNR data matches all the elements in a scenario. Targeting officers at the National Targeting Centre (NTC) conduct further research to either negate the risk or issue a target which will result in the passenger being referred for secondary examination upon arrival at the port of entry.

Background

Based on a recommendation from the Office of the Privacy Commissioner, the CBSA committed to establishing a governance framework for the review of scenarios for effectiveness and proportionality and to ensure that the scenarios did not unnecessarily impede the civil liberties or human rights of travellers.

Scenario Creation and Review

Scenarios undergo various levels of review throughout their development and maintenance. The NTC Targeting Intelligence Unit is responsible for making proposals for new or modified scenarios based on intelligence (i.e.: interdiction reports, intelligence briefs/bulletins, systems information), trends and patterns. All scenario recommendations list the supporting documentation to justify the reason for the scenario. Prior to creating the scenario in PAXIS, the proposal is reviewed by the Targeting Rules, Indicators and Scenarios (TRIS) Unit. This Unit provides guidance to the Targeting Intelligence Unit on which data elements would best capture

the identified risk and avoid possible scenario overlap. Once a scenario is activated, the TRIS Unit utilises a rigorous monitoring and maintenance framework through which performance is reviewed and documented.

On an ongoing basis to confirm compliance to program requirements, the Targeting Program Unit reviews the scenarios (Appendix A: Scenario Review Process) to ensure compliance to all privacy, legislative and regulatory requirements. Scenarios of concern are flagged and raised at the Targeting Program Management Committee (TPMC) monthly meeting for discussion of the human rights and civil liberties implications of the scenario. If it is determined that a scenario unnecessarily impedes the civil liberties, privacy or human rights of travellers, it will be either deactivated or modified.

CBSA Commitments

In order to protect the civil liberties and human rights of travellers, scenarios must not contain any sensitive data as defined by the *Canada-European Union Passenger Name Record Agreement (CAN – EU PNR Agreement)*, which was developed having regard to the relevant provisions of the *Canadian Charter of Rights and Freedoms* and Canadian privacy legislation. Sensitive data is any information that could reveal:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Information about a person's health or sex life

The CBSA must adhere to all legislation and regulations with regard to the restrictions on the use of PNR data elements defined in the *Protection of Passenger Information Regulations* (*PPIR*), the *Passenger Information Customs Regulations* (*PICR*) and the *2014 CAN – EU PNR Agreement on the transfer and processing of PNR data.*

The consolidated requirements of the *PPIR, PICR, 2014 CAN – EU PNR Agreement* and the strict program application guidelines can be found in the Directive Memorandum D1-16-3 *Guidelines for the Access to, Use, and Disclosure of Advance Passenger Information (API) and PNR Data*.

Minimal Privacy Intrusion

Sensitive PNR data elements are not permitted to be used in the targeting process. To minimize privacy intrusion, PNR data elements within a scenario cannot contain any information that may be considered sensitive data.

Scope of a Scenario

PNR data elements are strictly used for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime.

> *CAN – EU PNR Agreement*: ***Article 3 (1)*** *Canada shall ensure that the competent authority (CBSA) processes PNR data received pursuant to this*

> *Agreement strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime.*
>
> *PPIR* **4 (1)** Subject to subsections (2) to (5), an official of the Agency may, for the following purposes, have access to any passenger name record information that is retained: **(a)** to identify persons who have or may have committed a terrorism offence or a serious transnational crime.

Civil Liberties & Human Rights

Civil liberties are the rights and freedoms recognised specifically by Canada, as per the *Canadian Charter of Rights and Freedoms* and *the Canadian Human Rights Act*. These are the rights and freedoms that protect an individual from the state and which are underpinned by a country's legal system. These are the basic rights and freedoms granted to Canadian citizens as well as all foreign nationals on Canadian territory.

> Section 2 of the *Charter of Rights and Freedoms* guarantees everyone has the following fundamental freedoms: freedom of conscience and religion; freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication; freedom of peaceful assembly; and freedom of association.
>
> Section 15(1) of the *Charter of Rights and Freedoms* guarantees every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability.
>
> Section 3 of the *Canadian Human Rights Act* states that the prohibited grounds of discrimination are race, national or ethnic origin, colour, religion, age, sex, sexual orientation, marital status, family status, disability and conviction for an offence for which a pardon has been granted or in respect of which a record suspension has been ordered.

SBT Governance

The governance surrounding SBT leverages the existing targeting organizational framework to ensure it is effectively and efficiently managed and complies with international agreements and legislative requirements.

Traveller Scenario Management Committee (TSMC)

This Committee is responsible for conducting ongoing reviews of scenarios, scenario development, and management processes/procedures to ensure scenario effectiveness, development and management process/procedural efficiency, consistency and integrity. Scenarios deemed ineffective may be deactivated or modified, and processes/procedures are updated as required. The committee also reviews and finalizes potential scenario effectiveness assessment proposals/plans.

For further information, refer to the Terms of Reference (TOR) of the TSMC (Appendix B).

Targeting Program Management Committee (TPMC)

The mandate of this Committee is to ensure the management of the Targeting Program, including SBT, is efficient and effective, as well as operationally compliant with international agreements and legislative requirements. In order to achieve this, the TPMC leverages the existing organizational framework and ensures the necessary leadership, communications and processes in place.

For further information, refer to the TOR of the TPMC (Appendix C).

Enforcement and Intelligence Program Management Table (PMT) and Traveller PMT

Unresolved issues surrounding SBT are referred to the Enforcement and Intelligence PMT (refer to Appendix D for the TOR), the Traveller PMT or both as required. The Chair and Co-Chair of the PMT are accountable for providing guidance and direction to the responsible Directors as follows:

- Ensuring strategic planning and horizontal communications with regards to SBT.
- Providing guidance on implementing and monitoring performance measures.
- Identifying and leveraging best practices for SBT.
- Reviewing program costs and identifying opportunities for savings within SBT.
- Ensuring overall alignment with Agency priorities or long-term planning.

Roles and Accountabilities

Operations Branch, National Border Operations Centre, NTC

The NTC is responsible for the operational delivery of SBT, thereby making it accountable for the following:

- Maintaining the SBT operational procedures including scenario development, activation, monitoring, and performance reporting.
- Ensuring all SBT operational procedures, scenarios and other documentation are protected to align with CBSA security and policies.
- Training and communicating to all identified partners in the scenario creation process the standard operating procedures for scenario creation management, monitoring and compliance.
- Recording all intelligence used to build a scenario in addition to maintaining the scenario development tracking log and scenario master list.
- Retaining all targeting scenario proposal templates in addition to recording the activation, modification and deactivation of scenarios.
- Monitoring and tracking API/PNR data quality and consulting with internal partners regarding data provision issues that impact the effectiveness of scenarios or the efficiency of PAXIS.

- Leading the development of all scenarios composed in collaboration with internal and external/international partners.
- Developing and distributing SBT performance reports to internal stakeholders.
- Ensuring all individual scenarios meet legislative and privacy compliance requirements.
- Assuming the responsibility for the scenario lifecycle including scenario activation, modification, and deletion.
- Ensuring scenarios are operationally manageable and proportionate by assessing the scenario operational impacts prior to activation;
- Reviewing examination results, the risk environment and new trends to determine if the scenario should remain active, be modified or deactivated from PAXIS;
- Calibrating the effectiveness of scenarios through research and analysis, consultations with internal and external partners;
- Monitoring individual scenario effectiveness through performance metric analysis; and
- Utilizing and maintaining a detailed log to provide an auditable record of scenario compliance review.
- Coordinating and maintaining records of the TSMC.

Programs Branch, Enforcement and Intelligence Programs Directorate, Targeting Program Unit

The Targeting Program Unit is the functional authority for the targeting program, and is responsible for providing program strategy and policy direction related to SBT. Its accountabilities include:

- Maintaining the *Scenario Based Targeting Governance Framework*;
- Coordinating meetings and maintaining records of the Targeting Program Management Committee;
- Reporting and escalating issues on SBT related matters, as required;
- Supporting the NTC to initiate systems, tools, business and process improvements facilitating operational delivery and ongoing enhancement of SBT (i.e. new systems/applications, analytical tools and processes – e.g. SPSS modeller, data warehouse, etc.); and,
- Evaluating scenarios for potential impacts on civil liberties and human rights and raising any identified scenarios of concern to the TPMC (for more information, refer to Appendix D the "Scenario Review Guidelines").

Programs Branch, Traveller Programs, Air Programs Unit

The Air Programs Unit develops, amends, and maintains related legislations and regulations related to traveller processing in the air mode and is the Office of Primary Interest for PAXIS. Its accountabilities include:

- Providing program strategy and policy direction related to the collection and use of API/PNR;
- Developing and maintaining related policies, regulations, and legislation for the acquisition and use of API and PNR data;
- Controlling and approving requests for access to PAXIS; and,
- Coordinating targeting and API/PNR systems changes/fixes or projects in conjunction with Business Systems Integration Division.

Issue Escalation Process

When there is an identified issue dispute regarding the policy compliance or legislative authority to initiate a specific scenario, the Traveller Scenario Management Committee or its members will notify the co-chairs of the Targeting Program Management Committee as soon as practical.

Should the directors fail to reach consensus, a joint briefing to the relevant directors general and vice presidents (as required) will be initiated by the Director of Intelligence, Targeting and Criminal Investigations Program Management.

For all disputes regarding a scenario with imminent and significant national security or public safety implications, the scenario will either be activated or remain in PAXIS until such time as the dispute is resolved.

In all other cases the TPMC will inform the directors general of the scenario proposal and delay its implementation until it is has received director general level approval.

Appendix A: Scenario Review Process

The following is the CBSA process to ensure all activated or modified scenarios are reviewed and adhere to all privacy, legislative and regulatory requirements.

Notification

When a scenario is activated or modified, the Targeting Risk Indicators and Scenarios Unit (TRIS) informs the TPU by sending an encrypted email to the TPU general inbox documenting the Scenario Master List (SML) changes. The emails are kept as reference to ensure accountability of the process.

Frequency

The TPU general inbox is monitored daily to ensure all activated or modified scenarios are reviewed on an ongoing basis. The TPU will maintain a tracking sheet of the results of the scenario review and a report is produced quarterly.

Meeting Privacy, Legislative and Regulatory Requirements

The CBSA will review all individual scenarios to ensure they do not contain any sensitive data as defined in the *CAN – EU Agreement.* Each activated or modified scenario must meet all requirements identified in the *PPIR*, D1-16-3, Sections 2 & 15(1) of the *Charter of Rights and Freedoms* and Section 3 of the *Canadian Human Rights Act*.

The CBSA will review all individual scenarios to ensure the scope is limited to targeting high-risk travellers, who pose a risk to the safety and security of Canada through suspected involvement in terrorism, organized crime, or other serious crimes that are transnational in nature.

Tracking

After each scenario is reviewed, the results are documented on a tracking sheet maintained by the Targeting Program Unit.

Reporting

The tracking sheet will be shared with members of the Targeting Program Management Committee (TPMC) prior to being finalized. Any issues identified with respect to the review of scenarios and their potential impacts on privacy, civil liberties and human rights, will be discussed at the TPMC meeting amongst stakeholders.

Recourse

Issues that cannot be mitigated at the TPMC are escalated to senior management, with final oversight and approval handled by the Enforcement and Intelligence Program Management Team (E&I PMT).

Storage

Each finalized and approved quarterly report is stored by the targeting program in PDF format for internal and external purposes as required.

Appendix B: Terms of ReferenceTraveller Scenario Management Committee

---

Context/Background:

Scenario Based targeting (SBT) is a key part of the Canada Border Service Agency's (CBSA's) pre-arrival traveller targeting program and supports the Agency's Risk Assessment Program by contributing to the identification and interception of suspected potential high and unknown risk people that may pose a threat to the national security, safety and prosperity of Canada. It also fulfils a commitment made by the CBSA under the Beyond the Border Action Plan to implement an enhanced SBT targeting methodology similar to that of the US Customs and Border Protection.

Increasing targeting work volumes, finite resources, ongoing scrutiny of standardized/automated risk assessment and border security approaches and ever-changing risks/threats necessitate ongoing robust rigour and scrutiny of the CBSA's risk management and assessment tools such as pre-arrival targeting's SBT process.

At the heart of SBT are the scenarios. In order to ensure the integrity and effectiveness of SBT and the overall success of the CBSA's traveller targeting program, the effectiveness of scenarios and the efficiency and integrity of their development and management processes/procedures needs to be regularly reviewed and adjustments made as required.

Prior to the Programs Branch realignment in June 2014, Targeting Programs was responsible for SBT scenario development/implementation, management/maintenance, monitoring. Responsibility for all these activities was transferred to the National Targeting Centre (NTC) - Operations Branch as part of the realignment. Targeting Programs provides oversight for the CBSA's Targeting Program.

Mandate/Expected Outcome

Conduct ongoing review of scenarios and scenario development and management processes/procedures to ensure scenario effectiveness, development and management process/procedural efficiency, consistency and integrity. Scenarios deemed ineffective may be deactivated or modified, and processes/procedures will be updated as required. The committee will also review and finalize potential scenario effectiveness assessment proposals/plans.

Initially will include applicable NTC team representatives, but will be expanded to include Targeting/Intelligence Programs and Intelligence Operations and Analysis Directorate (IOAD), and other areas as required. Guests (e.g. IT) will be invited to speak to specific topics as required.

Chair – NTC	**Paul Porrior, Director**
Co-Chair: NTC	**Curtis Young, TRIS Manager**
Secretariat:	**Targeting Rules Indicators and Scenarios (TRIS)**

Representatives

NTC:

NTC – Targeting Intelligence (TI)	Tom Toulouse, Francesca Macchione, David Whetstone
NTC – Traveller Targeting (TT)	Marc Beauvais, Philip Crabbe, Natalie Rocque
NTC – TRIS	Kelly Cummings, Lauren Berrigan
NTC- Data Analytics Unit (DAU)	Mohamed Migahed
Targeting Programs	Melissa Wigham; Jo-Ellen Langevin

*Members require Secret clearance and a working knowledge of SBT.

Meeting Frequency

Monthly

Members Roles and Responsibilities

- Review scenarios for effectiveness and make recommendations for deactivation or modification as appropriate.
- Review and finalize scenario effectiveness assessment proposals/plans.
- Review and make amendments to scenario development and management processes and procedures as required.
- Disseminate information/recommendations to their respective areas, as required.
- Share scenario development best practices and lessons learned.
- Discuss issues that impact the SBT process (ex: data quality, provision, review rates, scenario capacity limit, elements for coding).

TRIS

- Draft proposals for scenario effectiveness assessments
- Present findings on scenario effectiveness.
- Lead scenario review, effectiveness assessment proposal and process improvement discussions.
- Present items for discussion.

Meeting Organization

- Working group meetings will be held once a month for approximately 2 hours. May be held more often as required.
- Selection of scenarios for review and associated performance analysis reports will be prepared by TRIS for discussion at the meeting.
- Records of discussion will be drafted and shared by the Coordinator.

Appendix C: Terms of Reference Targeting Program Management Committee

Mandate

To ensure the management of the Targeting Program is efficient and effective, as well as operationally compliant with international agreements and legislative requirements. In order to achieve this, the Targeting Program Management Committee (TPMC) will leverage the existing organizational framework and will strive to have the necessary leadership, communications and processes in place.

Membership

Chair:

Director of Intelligence, Targeting and Criminal Investigations Programs Management Division and

Director of the National Targeting Centre

Note: Director of Program Compliance and Outreach, Commercial Programs, will be an additional co-chair for TPMC-commercial meetings only

Secretary:

Targeting Program Unit (TPU)

Members:

To include Managers and Senior Program Advisors from the following areas:

Operations Branch:

- Commercial Operations Division
- National Targeting Centre
- Intelligence Operations and Analysis Division
- Traveller Operations Division

Programs Branch:

Commercial Program and Policy Management Division

Commercial Program Compliance and Outreach Division

Intelligence, Targeting and Criminal Investigations Programs Management Division

Program Business Systems Integration Divisions

Traveller Program and Policy Management Division

Note: Other areas may be invited to attend meetings on an ad-hoc basis dependent upon specific agenda items.

Authority

The Co-Chairs of the Committee have the authority to set the overall strategic direction of the Committee, to approve Committee agendas, and to request items be brought forward at a specified date.

The Co-Chairs retain the decision-making authority as to when to escalate items put before the Committee if consensus cannot be achieved; however, the Co-Chairs shall seek to build consensus among members in carrying out this duty.

Roles and Responsibilities

To fulfill its mandate, the Committee will:

- Receive a briefing from the Scenario Management Committee (SMC) meetings (for TPMC-traveller meetings only)
- Receive a briefing from the Commercial Risk Capability Management Committee (CRCMC) Committee meetings (for TPMC- commercial meetings only)
- Monitor and periodically review:
    - SBT scenarios / commercial risk rules
    - Targeting performance measurement, budget planning and accountability requirements
    - Data quality issues
    - Industry data submission compliance rates
    - Effectiveness of National, Regional, Internal Intelligence in support of the National Targeting Model
- Develop, review or recommend targeting policy, procedures, guidelines, processes and system requirements.

- Identify, analyze and propose solutions for any issues that have an impact on the delivery of the Targeting Program such as Human Resource planning, recruitment processes and training.

- Identify, analyse and propose solutions for any issues that have a direct impact on the success of the Targeting Program, such as the essential "inputs" (National, Regional, Internal Intelligence, data (internal, external), Exam Results (closing the loop), Partnerships (GoC, International)), as identified in the Internal Audit and Program Evaluation.

- Provide reporting and recommendations to the Directors of the NTC, E&I Programs Management, Traveller Program and Policy Management, and Commercial Program and Policy Management concerning outstanding issues and/or achievements.

Meeting Frequency:

Separate committees will be held for commercial and travellers streams during the last week of each month. It is anticipated there will be a joint commercial-travellers TPMC held two times a year to discuss cross-cutting issues in a consolidated forum.

Record of Discussion and Decision:

The Secretariat of the Committee is responsible for drafting and disseminating a Record of Discussion and Decision (RoDD) to all attendees within three (3) business days after a meeting is held.

Escalation:

The Co-Chairs are responsible for escalating, to the appropriate parties, any issues emanating from the meeting within three (3) business days after a meeting is held.

Proxies to meetings:

Members of the Committee shall nominate a proxy to attend a meeting if the member is unable to attend. Proxies are expected to brief all affected parties within their Unit, Division and Directorate on all decisions made at the Committee.

Please note that membership is recommended to be at the Manager and Senior Advisor level. Proxies should be first at the Senior Advisor level and if neither the Manager nor Senior Advisor is available, a Senior Program officer can represent their area.

Quorum Requirements:

A minimum of four (4) committee members is required for the meeting to be recognized as an authorized meeting. If either of the Co-Chairs or their representatives are unavailable, the scheduled meeting may be cancelled or rescheduled.

Appendix D: Terms of Reference Enforcement and Intelligence Program Management Table

Membership

The Enforcement and Intelligence Program Management Table (EI PMT) members will consult jointly and provide integrated and functional guidance to the following eight (8) EI programs: Intelligence, Targeting, Security Screening, Criminal Investigations, Immigration Investigations, Detentions, Hearings and Removals. The Intelligence Program also includes some areas under International Region and the National Targeting Centre.

This PMT is a focussed, action-oriented decision making body and is responsible for providing leadership on the EI's program strategic policy direction, priority setting, performance measurement, risk identification and mitigation strategies, workforce training and learning requirements and making financial recommendations.

Membership

Chair	• Director General, Enforcement and Intelligence Programs Directorate, Programs Branch
Deputy Chair	• Director General, Enforcement and Intelligence Operations Directorate, Operations Branch
Secretariat	• Director, Program Performance, Reporting and Transformation Division, Enforcement and Intelligence Programs Directorate, Programs Branch

Appendix D: Terms of Reference Enforcement and Intelligence Program Management Table

Standing Members	• Executive Director, Enforcement & Intelligence Programs, Programs Branch • Director General, Global Border Management and Data Analytics, Programs Branch • Director General, International Region, Operations Branch • Executive Director, Pacific Region, Operations Branch • Director General, Training and Development, Human Resources Branch • Director General, Corporate Planning and Reporting, Corporate Affairs Branch • Director General, Enterprise Architecture and Information Management, Information, Science and Technology Branch • Director General, National Border Operations Centre, Operations Branch • Director, National Targeting Centre, Operations Branch • Director, Strategic Finance and Costing, Comptrollership Branch • Directors, Enforcement and Intelligence Programs, Programs Branch
Required Participants	• Senior Advisor, Programs and Operations Communications, Corporate Affairs Branch • Manager, Strategic Finance and Costing, Comptrollership Branch • Senior Program Advisor, Governance and Financial Oversight Unit, Enforcement and Intelligence Programs, Programs Branch
Ad Hoc Members*	• Directors, Enforcement and Intelligence Operations, Operations Branch • Directors, International Region, Operations Branch • Directors, National Border Operations Centre, Operations Branch • Director, Business Systems Integration (E&I support), ISTB Branch **Based on the agenda items, attendance to the PMT will vary for Ad Hoc Members**

Note: Each Standing Member of the EI PMT shall nominate one proxy at the Director level to attend meetings in the event that the Member is unable to attend. Every effort should be made by each Standing Member to attend all meetings. Every effort should also be made to ensure that a proxy is available for all meetings that the Standing Member is unable to attend, and is well briefed on the operations of the PMT. Subject matter experts and observers may be invited to attend a PMT meeting at the Chair's discretion.

Responsibilities and Duties

The EI PMT has the responsibility for decisions that affect the functional direction and oversight, budget management, and monitoring and performance reporting of the Enforcement and Intelligence Programs. To do this, the EI PMT will focus on the following areas:

1. Serve as an active and dynamic oversight body with regards to financial, budgetary, training and learning, and human resource planning issues, and provide input on the PMT's forward agenda.

2. Support vertical and horizontal communications and engagements and seek to build consensus among Standing Members and Ad Hoc Members.

3. Provide strategic direction for EI stakeholder engagement, including (a) form and dissolve EI level committees, and (b) establish reporting requirements for committees. These committees will then analyze/examine and propose resolutions and report back their findings to the EI PMT.

4. Ensure alignment of identified priorities and evaluate performance measurements on a quarterly basis.

5. Report to the President on the PMT progress on established performance indicators and make recommendations relating to Criminal Investigations, Immigration Enforcement Program Activities and Targeting, and the Intelligence and Security Screening Program Sub-Activities, in collaboration with the Program Policy Committee (PPC) and Executive Committee (EC).

6. Provide direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

Chair

The duties of the Chair of the EI PMT are an extension of his or her organizational responsibilities as the DG of the Enforcement and Intelligence Programs Directorate.

1. Serve as the single point of accountability for the PMT, as well as the decision-making authority on items put before the PMT.

2. Retain the sole authority to make a decision to escalate issues to the Program Policy Committee (PPC) for consideration, resolution, and/or guidance.

3. Responsible for vertical and horizontal communications and engagement.

4. Establish a results measurement framework for monitoring the PMT's performance, while evaluating progress on a quarterly and annual basis.

5. Facilitate meaningful and effective meetings, ensuring that items brought to the PMT have been broadly and adequately consulted.

6. Determine PMT membership in collaboration with the Deputy Chair.

7. Responsible for providing direction to the PMT Secretariat for all corporate and logistical matters to ensure effective and efficient PMT meetings.

8. Delegate duties and oversight of certain areas of responsibility to the Deputy Chair.

Deputy Chair

1. Assume the roles and responsibilities of the Chair in the Chair's absence, as well as other duties and responsibilities as assigned by the Chair.

2. Collaborate with the Chair in determining PMT membership.

3. Build consensus with the Chair, on key issues and decision points before and after PMT meetings, to address contentious issues, potential conflicts of interest and work towards integrating program and operational activities to achieve the best results possible.

4. Consult with senior management in the Regions and represent their views to the extent possible at EI PMT meetings, while reporting back to them on all PMT business.

Governance Structure

The EI PMT is accountable to the Program Policy Committee (PPC). The role of the PPC is to advise Executive Committee (EC) on strategic policy and ensure the ongoing development of CBSA policy and program delivery and to identify and manage functional management issues in relation to risk.

The PMT is the governing authority for director-level committees and managerial program committees. Director level committees are:

- National Inland Enforcement Committee,
- National Intelligence, Targeting and Security Screening Committees, and
- National Criminal Investigations Committee.

Committee membership is composed of both Headquarters and regional members.

Managerial working level groups should exist for all EI Programs. Managerial level working group membership is composed of the program's respective national managers and regional managers.

It is expected that issues will be brought forward at the appropriate working level and follow the governance hierarchy in seeking approvals by, or providing briefings to, the relevant decision-making body. Director level committees may additionally wish to seek approval or consult with the EIOD Directors/DG Operations Committee on relevant issues.

The committees and working groups meet on a regularly scheduled basis and report to the PMT bi-annually on issues such as risk/risk mitigation, performance and financial management by undergoing a Program Health Check. The Program Health Check ensures regular governance oversight by the Table and provides an opportunity for program managers to seek guidance or socialize key program management or policy issues.

Please see Appendix A for further details on the EI PMT Governance structure and Program Health Check calendar.

Table Operation

Frequency and Duration

The EI PMT shall meet on a monthly schedule on Wednesdays, or more frequently if required. *Ad hoc* meetings may be scheduled as required at the request of the Chair.

Quorum

A minimum of four EI PMT Standing Members, including the Chair or the Deputy Chair, are required for the meeting to be recognized as an authorized meeting.

Materials and Records of Discussion

The EI PMT Secretariat will prepare the Agenda and the Record of Discussion (RoD) for each meeting and provide to the Chair for final review and approval. The RoD shall include clear action items, with assigned leads and Brought Forward (BF) dates. It will also include standing and forward agenda items. The Secretariat is responsible for disseminating the RoD to all Standing Members prior to the next meeting. RoDs and Annexes will be made available to EI PMT Members as needed in an effort to promote information sharing. The RoD and identified action items from each meeting will be maintained and monitored by the Secretariat.

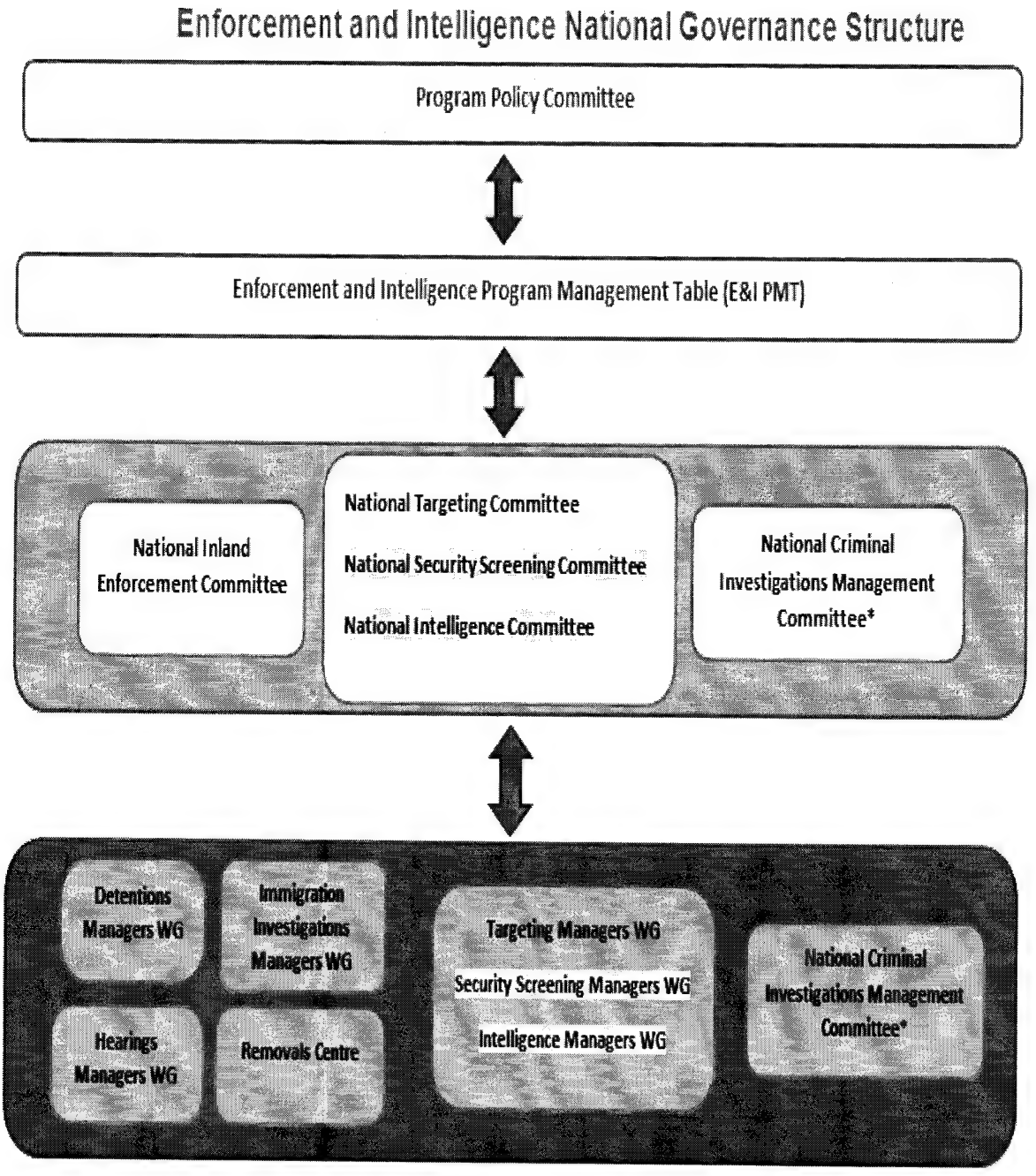
The Chair shall finalize and approve the agenda for each EI PMT meeting one week before the scheduled meeting. Materials are normally available to EI PMT Members two business days in advance of any meetings.

Appendix D: Terms of Reference Enforcement and Intelligence Program Management Table

Values Based Leadership and Organizational Culture

EI PMT Members, through their actions and words, shall demonstrate their commitment to the highest standards of integrity, ethical values and professionalism in the performance and functional management of programs.

Appendix D: Terms of Reference Enforcement and Intelligence Program Management Table



January 2016

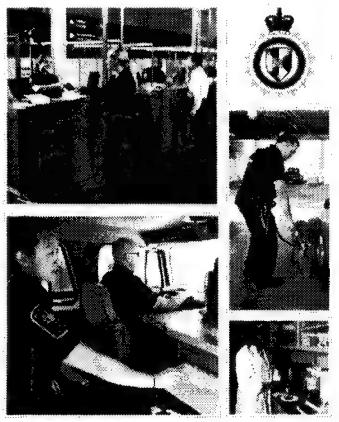
Yellow: in development ; * combined manager/director committee

CBSA ASFC

PROTECTION - SERVICE - INTEGRITY PROTECTION - SERVICE - INTÉGRITÉ

Canada Border Services Agency (CBSA)

Targeting Program - Traveller



July 23, 2014

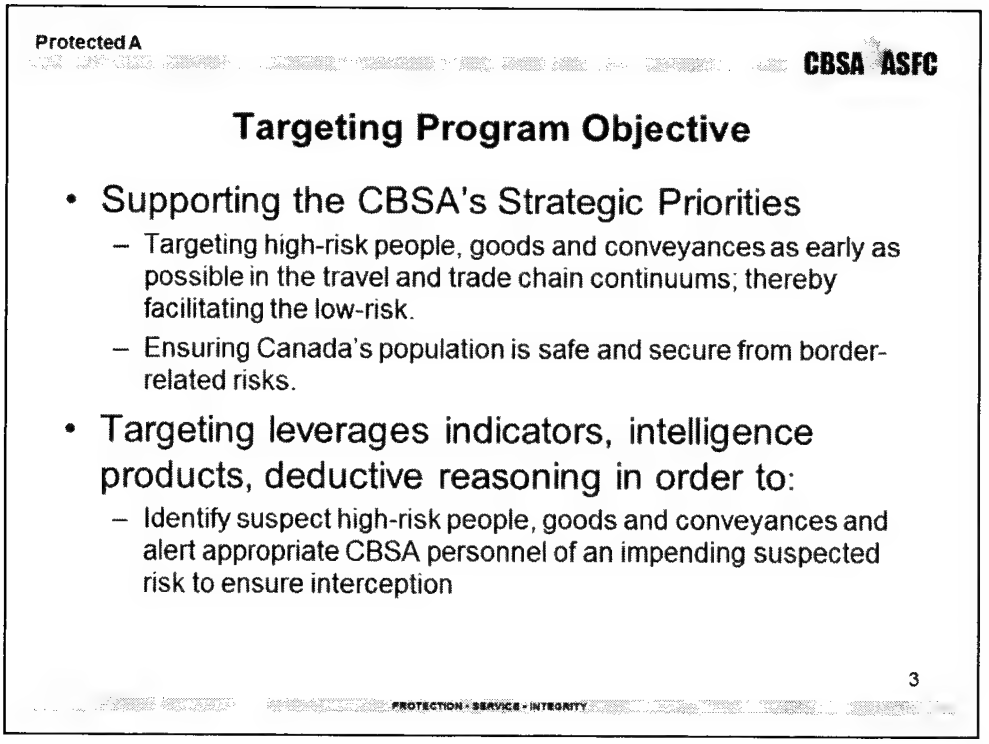
Canada Border Services Agency | Agence des services frontaliers du Canada

Canada

CBSA ASFC

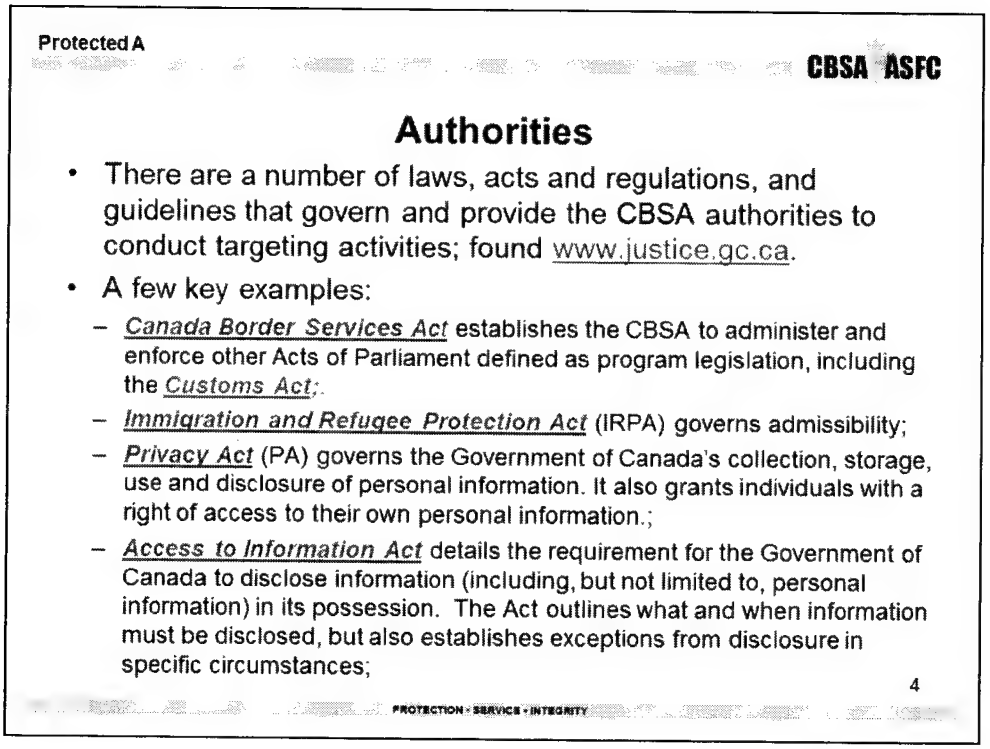
Overview

- Targeting Program Objective
- Authorities
- Targeting Cycle
- Targeting Process
- Centralized Targeting Business Model
- National Targeting Centre (NTC)
- Targeting Program Unit – Key Activities
- Future – Traveller
- Challenges
- Questions



Objective:
The CBSA has been conducting targeting-related activities for over 30 years. Over this time, the program has proved invaluable to border management by supporting national security and public safety priorities.

Support for CBSA's priorities:
The CBSA Targeting Program significantly contributes to the detection and interception of high-risk people, goods, conveyances and crew that may pose a threat to the security of Canada and the North American perimeter.



The *Customs Act* (CA) establishes the requirements for presenting and reporting to the CBSA. This includes reporting of goods and conveyances imported to, and in some cases, exported from Canada, as well as the requirements for the presentation of persons entering Canada. In some circumstances, the *Customs Act* requires the submission of advance information for a conveyance, person or good to the CBSA prior to their arrival in Canada. The *Customs Act* also contains specific and strict provisions regarding the use and the disclosure of "customs information." (See in particular sections 11. (1), 12. (1) to (3), 12.1, 95. (1) to (4), 107.1)

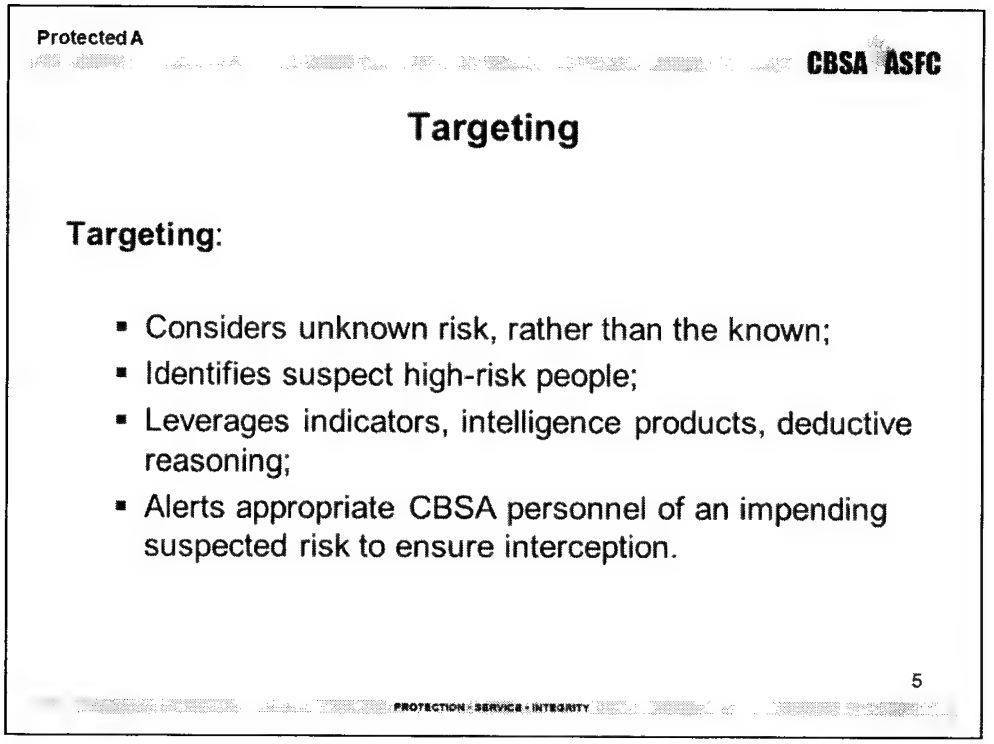
SOME RELATED REGULATIONS:

- *Protection of Passenger Information Regulations* (PPIR) governs the use, retention, access and disclosure of API/PNR information.
- *Passenger Information (Customs) Regulations* require commercial carriers, charterers, travel agents, and owners and operators of a reservation system to provide the CBSA with or to provide the CBSA with access to, specific information related to persons entering Canada. The regulations clearly outline what is required to be reported to the CBSA and indicates the format in which that information is to be provided. (See in particular sections 2, 3, 4)

- *Immigration and Refugee Protection Regulations* (IRPR) contain regulations that are relevant to this policy, in particular those which state that commercial transporters must provide advance passenger information for each person carried. These regulations apply to the air, marine and rail modes of transportation. (See in particular sections 269 (1) and (2))

ALSO, the Agency develops memoranda that interprets legislation and regulations, and their application, for the use of the public and Agency personnel, such as:

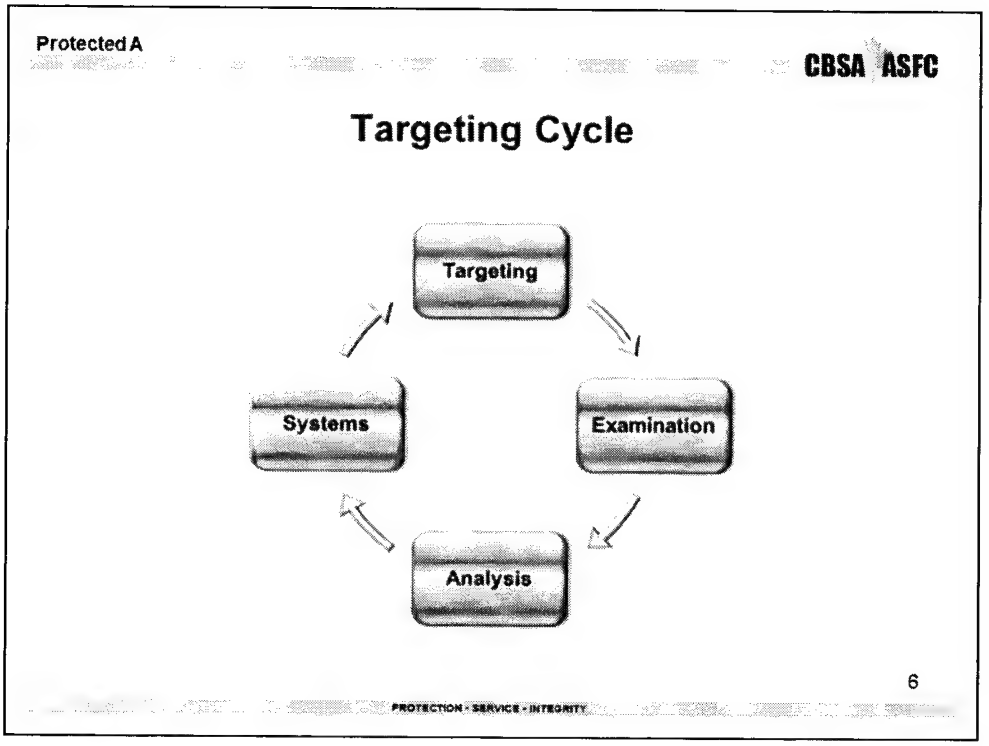
D-Memo 1-16-3 Administrative Guidelines for the Provision to Others, Allowing Access to Others and Use of Advance Passenger Information (API) and Passenger Name Record (PNR) Data



Targeting – Targeting is the process of identifying suspect high-risk people, goods and conveyances through a deductive reasoning process utilizing advance information, technology and intelligence products.

Target – A target is a type of referral using advance information that identifies suspect high-risk people, goods and conveyances that may pose a risk to national security and/or public safety priorities

Air traveller targeting in particular is based on receipt of advance information, and is conducted prior to a traveller's arrival in Canada. This activity relies on good quality data received in a timely fashion; that is, prior to the traveller's arrival in Canada.



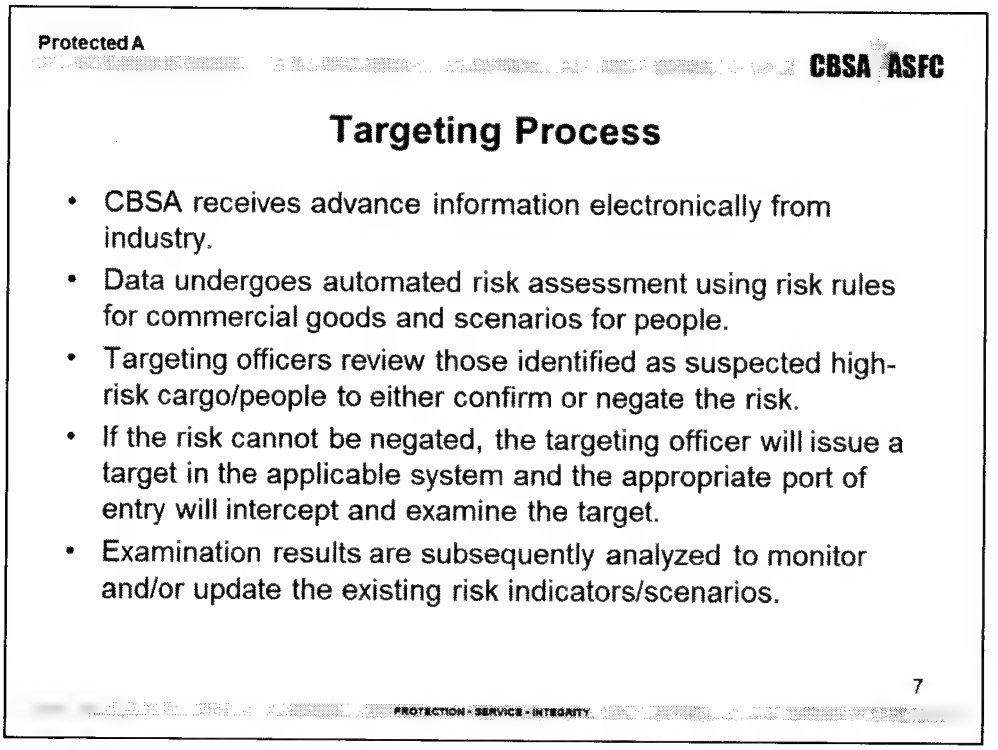
Systems: The cycle begins when advance information received by the CBSA is queried against the risk rules and scenarios in an automated process to assist the targeting officers in identifying high-risk people, goods and conveyances.

Targeting: The targeting officer uses information contained in various systems, known risk indicators/scenarios and intelligence, combined with deductive reasoning and critical thinking skills, to identify suspected high-risk people, goods or conveyances and issues targets into appropriate targeting systems for interdiction.

Examination: Targets are intercepted and examinations of suspected high-risk people, goods or conveyances are conducted by border services officers. Results of those examinations are documented and reported in the prescribed manner according to the mode.

Analysis: CBSA analyzes examination results to support the targeting community. Indicators, risk rules, and scenarios are adjusted or new ones are identified and the automated risk assessment systems' data is updated ensuring this information is fed back into the Targeting Cycle. This "closing of the loop" is critical to the targeting cycle, as it either confirms effectiveness of risk rules and

scenarios, or identifies where areas of opportunity exist.



These steps outline the general targeting process.

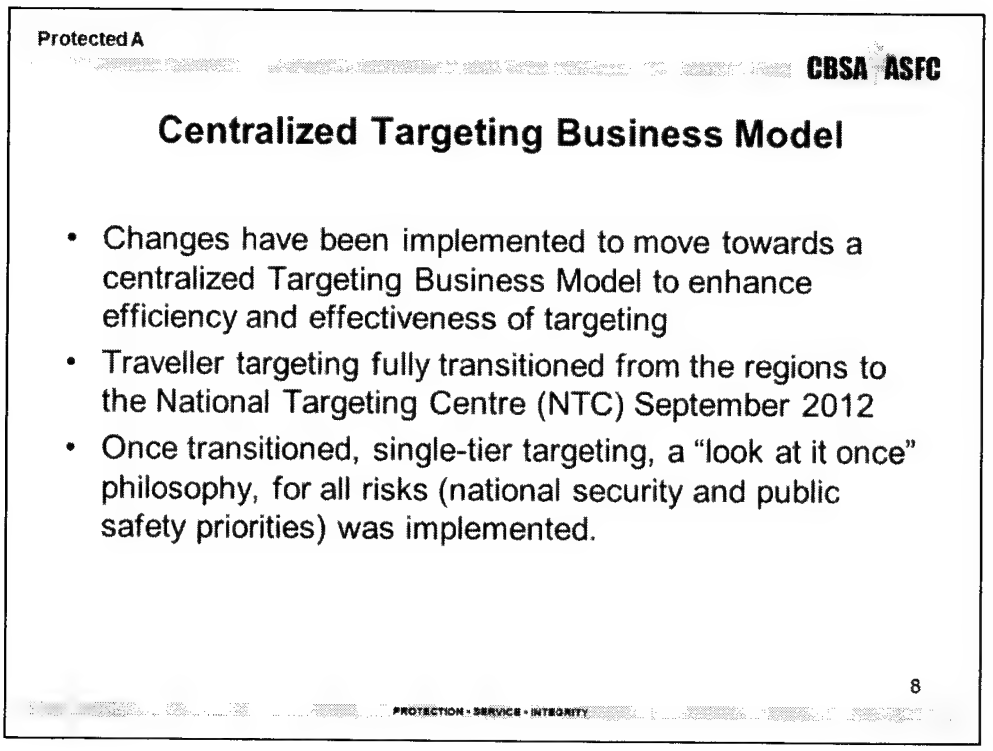
1. CBSA receives advanced information electronically from airlines and service providers

2. The data is assessed against enforcement information as well as scenarios to identify known and potential risks

3. When there are matches, the traveler information is presented to a targeter who then reviews the information to confirm or negate risk.

4. If the risk cannot be negated, the targeting officer will issue a target and bring this to the attention of the appropriate port of entry for their interception and examination upon arrival

5. All examination results are then reviewed to monitor or update the scenarios.



The CBSA elected to implement a centralized targeting business model in order to enhance the efficiency and effectives of targeting. The National Targeting Centre here in Ottawa was chosen as the central location for many targeting activities. Over time, all targeting activities will be handled through this site.

Prior to centralisation, traveler targeting was handled individually by the major Canadian airports. While the activities were similarly handled in each airport, the techniques employed at these various locations varied, as did the results/effectiveness, efficiencies, reporting and communications/linkages to the relevant areas of the Agency.

Canada Border Services Agency | Agence des services frontaliers du Canada

Cover Sheet for New Initiatives Submitted for Programs Branch Prioritization

Date Submitted to Business Planning and Resourcing Division :

22SEP2010

ABOUT THE INITIATIVE

New Initiative Subject	**Programs Branch Division**
Long Term Technical Solution for Scenario Based Targeting in PAXIS	Targeting and Risk Management Division, Risk Assessment Programs Directorate

Description of the Initiative

A consultation report outlining the technical options and costing for a long term solution was completed by Enterprise Architecture in August 2009. An approval decision for fully functional Scenario Based Targeting within PAXIS was provided by the Executive Policy Committee in January 2010. The Committee was very supportive of the proposal and discussed how best to quickly bring it to the attention of the Deputy Minister of Public Safety, the National Security Agency (NSA) and the Minister. Finally, the Committee focused on the need to firm up the costing figures and Innovation Science and Technology Branch confirmed that should this project go ahead, they would treat it as a priority with a view to implement in 2011. In order to support the new Targeting Service Delivery Model based on Strategic Review, a long term solution must be in place by March of 2012.

The original costing for this option will need to be reconfirmed by all parties. Business requirements have been adjusted slightly due to the assumption that some work initially costed in the consultation will have been completed in the medium term solution, as well as some new and adjusted requirements being identified to support the new targeting model which comes out of strategic review. A funding source has not yet been identified. Clear costs must be identified prior to requesting funding.

Scenario-Based Targeting is currently listed as Priority 5 to have costing conducted by Portfolio Management and requires higher priority in order to meet international commitments and Targeting Service Delivery Model requirements.

Detailed Business Requirements will be forwarded as soon as possible.

Indicate which of the following previously identified priorities the initiative corresponds to, if applicable.

- ☒ Strategic Review
- ☐ Minister's Mandate
- ☐ Cabinet Commitments
- ☐ Commitments to Business Community
- ☐ Change Agenda

If the initiative does not relate to one of the commitments mentioned above, please indicate how the initiative relates to any other Agency priorities.

Have any commitments been made about this initiative? Please indicate the commitment and whether it was made internally or externally.

Commitments during MOU negotiations and revision meetings committed that CBSA would move forward quickly to implement full scenario based targeting capability. The current agreements and MOU were adjusted to accommodate these expected changes. As per commitments within the Targeting Service Delivery Model (Strategic Review)

What are the high level benefits of going forward with this initiative?

Originally, as part of the presentation to EPC, implementation of a long term technical solution was impacted for completion in 2011. Original impact suggested that one year was required for development and implementation. Once a funding source is identified, time commitments will need to be revisited.

Though not announced, this initiative would need to be implemented prior to March 2012 in order to fully support the benefits of the Targeting Service Delivery Model resulting from Strategic Review.

What are the high level impacts of not going forward with this initiative?

The implementation of fully functional scenario based targeting within PAXIS is required to support the new targeting model resulting from Strategic Review. The risk scoring program is, and will continue to be, ineffective in identifying incoming air travellers as potential high-risk travellers if left as status quo.

The medium term technical solution will only automate a limited number of scenarios with little or no capability to add or adjust rules. In order for CBSA to be able to respond to world events and intelligence trends, further functionality is required.

Impacts of not implementing a long term scenario based targeting solution will hinder other initiatives such as API/PNR expansion to include rail and marine passenger targeting, as well as possible hindering targeting requirements for postal mode as well as commercial.

If full functionality of scenario-based targeting is not implemented, this will negatively impact CBSA's ability to support the targeting service delivery model that was committed to as part of Strategic Review.

COSTING INFORMATION

Has a source of funding been identified?	**Please describe your identified source of funding, or the proposed source.**
☐ Yes ☒ No	

Has any costing been done on this previously?	If costing has previously been done, please indicate when the costing was done and provide details about the costing.
☒ Yes ☐ No	Yes – Costing was conducted in 2009 as part of a consultation conducted by enterprise Architecture. Since that time, business requirements have been adjusted slightly due to the assumption that some work initially costed in the consultation will have been completed in the medium term solution, as well as some new and adjusted requirements being identified to support the new targeting model which comes out of strategic review. A funding source has not yet been identified. Clear costs must be identified prior to requesting funding.
Has a work order (WO) for costing purposes been opened yet? ☐ Yes ☒ No	**If yes, indicate the WO number and when it was opened.**

ADMINISTRATION

Program Director	Division	Phone Number
Jo-Anne Drewniak	Targeting and Risk Management Division	(613) 948-8156
Director General	**Directorate**	**Phone Number**
Lorne Lawson	Risk Assessment Programs Directorate	(613) 952-8655
Main Contact / Title	**Team**	**Phone Number**
Melissa Wigham – Manager	Risk Rules and Indicators- People and Goods	(613) 948-7122
Date Costing is required by:	**Please indicate the driver for this date:**	

TO BE COMPLETED BY THE BUSINESS PLANNING UNIT

Date Received by BPU	Date for discussion at BMT	Approved to go forward to ISTB : ☐ Yes ☐ No
Additional Notes/Comments		